4/2017

Datenschutz Nachrichten

40. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Die Datenschutz-Grundverordnung aus Sicht der Gesundheitsversorgung ■ Medizinforscher und Datenschützer fordern Bund-Länder-Staatsvertrag ■ Sensorik, automatische Entscheidungen und Persönlichkeitsschutz ■ Nachrichten ■ Rechtsprechung ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt



Termine



Donnerstag, 01. Februar 2018
Redaktionsschluss DANA 1/2018

Samstag, 24. Februar 2017
DVD-Vorstandssitzung
Bonn, Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Freitag, 20. April 2018, 18:00 Uhr
Big Brother Awards
Bielefeld, Hechelei
https://bigbrotherawards.de/

Samstag, 21. April 2018
DVD-Vorstandssitzung
Bielefeld,
Anmeldung in der Geschäftsstelle
dvd@datenschutzverein.de

Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
40. Jahrgang, Heft 4

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Thilo Weichert
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0) 91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Kalenderjahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, AdobeStock, ClipDealer

Editorial

Datenschutz im Gesundheitsbereich

Jamaika kommt nun wahrscheinlich doch nicht; alles läuft auf Groko oder SPD-Tolerierung einer CDU-Minderheitenregierung hinaus. Für den Datenschutz sind das keine erfreulichen Perspektiven: Der schwarz-rote Mehltau, der inzwischen den offiziellen Datenschutz in Deutschland überzieht, droht beständiger zu werden als uns lieb sein kann.

Als schwarz-gelb-grün noch im Raum stand, die Zwischenergebnisse aber nicht erkennen ließen, dass es trotz FDP und Grünen ein Ruck beim digitalen Grundrechtsschutz geben würde, hat sich die DVD an einem offenen Brief beteiligt, in dem ein Ende der TK-Vorratsdatenspeicherung gefordert wurde.

https://www.datenschutzverein.de/wp-content/uploads/2017/10/2017-10-30-Pressemitteilung_offener_Brief_Jamaika.pdf

Zum Ende der Verhandlungen gab es insofern anscheinend Bewegung, auch wenn nicht alle Signale nur positiv waren. Jetzt dürfte der Datenschutz in schwarzer Hand bleiben. Dies bedeutet: Positive Tendenzen in Europa werden weiterhin gebremst. Datenschutz wird bürokratisch betrieben. Von Deutschland gehen keine Innovationen aus.

Diese Innovationen bleiben dringend nötig, insbesondere wo die DSGVO durch Öffnungsklauseln den EU-Mitgliedsstaaten Regelungsspielräume lässt. Ein solcher Bereich ist die Gesundheitsdatenverarbeitung, weshalb sich hier mit der DSGVO nicht so viel ändern wird. Bernd Schütze beschreibt die aktuelle Rechtslage unter Berücksichtigung der neuen BDSG-Regelungen. Damit bleibt nicht nur das Regelungschaos bestehen, es wird durch die weitere europäische Regelungsebene noch komplizierter. Dies ist für Anwender eine Zumutung, insbesondere für medizinisch Forschende, von denen keine Gesetzesexegesen erwartet werden können. Um diesen Missstand zu beseitigen, wurde von Kiel aus, u. a. mit Prof. Michael Krawczak, eine Initiative für einen Bund-Länder-Staatsvertrag zur medizinischen Forschung gestartet. Die Reaktion der Praktiker hierauf war bisher durchgängig positiv, die der Politiker tendierte gegen Null. Es bringt eben keine Wählerstimmen und keine Pressemeldungen, wenn man sich mit überfälligen, vernünftigen, aber nicht spektakulären Vorschlägen zur Verbesserung der Datenschutz-, der Gesundheits- und der Wissenschaftslandschaft befasst. So war es auch fast schon ein Wunder, dass die langgeforderte Einbeziehung der IT-Dienstleister von Ärzten und anderen Berufsgeheimnisträgern in den Schutzbereich der Schweigepflichtigen – fast im Verborgenen – zum allerletzten Drücker der letzten Legislaturperiode realisiert wurde.

Nötig ist mehr. Damit befasst sich der Beitrag zur Sensorik. Wenn Gedanken und Gefühle digital erfasst werden, darf das die Politik nicht kalt lassen. Dass die Googles und Facebooks dieser Welt sich unserer innersten Vorgänge bemächtigen, spielte bisher für die Politik nur dann eine Rolle, wenn dadurch Wahlen beeinflusst werden. Dabei darf es nicht bleiben.

Nachdem die letzte DANA 3/2017 übermäßig üppig geraten ist und spät ausgeliefert wurde, nun eine schlankere Nummer, die in ruhigen Winterabenden konsumiert werden kann. Viel Spaß und Erkenntnis dabei.

Thilo Weichert, DVD-Vorstandsmitglied

Autorinnen und Autoren dieser Ausgabe:

Dr. Bernd Schütze
Langjähriger Experte im Bereich Datenschutz und IT-Sicherheit,
schuetze@medizin-informatik.org

Prof. Dr. Michael Krawczak
Leiter des Instituts für Medizinische Informatik und Statistik an der Christian-Albrechts-Universität zu Kiel, imis@medinfo.uni-kiel.de

Dr. Thilo Weichert
Vorstandsmitglied in der DVD, Netzwerk Datenschutzexpertise,
weichert@datenschutzverein.de, Kiel

Bernd Schütze

Die Datenschutz-Grundverordnung aus Sicht der Gesundheitsversorgung

„Im Prinzip bleibt es, wie es ist“, dies war die Botschaft, welche die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Frau Andrea Voßhoff, 2016 in ihrem Grußwort auf dem BvD-Verbandstag 2016 verkündete. Eigentlich muss man sagen, dass das Prinzip des Verbots mit Erlaubnisvorbehalt zur Verarbeitung personenbezogener Daten gleichbleibt. In diesem Beitrag wird aus Sicht der Gesundheitsversorgung dargestellt, wie sich die Datenschutz-Grundverordnung (DS-GVO) auf die Akteure in der Gesundheitsversorgung darstellt. Dazu werden zunächst die Rahmenbedingungen betrachtet, anschließend einige ausgewählte Aspekte der DS-GVO angesehen.

Rahmenbedingungen: Alter Wein in neuen Schläuchen?

Datenschutzrechtliche Schutzziele

In § 1 Abs. 1 Bundesdatenschutzgesetz (BDSG) wird der Zweck des Gesetzes darin beschrieben, dass das BDSG den Einzelnen davor schützen soll, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht nicht beeinträchtigt wird. Unter der aktuell geltenden Gesetzeslage ist das datenschutzrechtliche Schutzziel also der Schutz des Betroffenen vor Beeinträchtigungen.

Die DS-GVO adressiert entsprechend Art. 1 drei Schutzziele:

1) Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten,
2) Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten,
3) Schutz des freien Verkehrs personenbezogener Daten in der Union, wobei der freie Verkehr aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden darf.

Unter der DS-GVO geht es also nicht länger darum, den Betroffenen vor Beeinträchtigung zu schützen. Die DS-GVO erlaubt eine Beeinträchtigung des Betroffenen, nur muss der Betroffene wissen, worum es geht. Um ein Bild zu gebrauchen: Das BDSG will verhindern, dass ein Mensch von der Brücke springt und dabei zu Schaden kommt, die DS-GVO möchte den Sprung nicht verhindern, jedoch soll der Mensch vor dem Sprung wissen, wie tief es ist und ob ihn unten Beton oder Wasser erwartet.

Konzernprivileg

Auch in der Gesundheitsversorgung gibt es diverse Konzerne, z. B. im Bereich der Pharmaindustrie oder bei privaten Klinikketten. Dementsprechend zeigte man sich auch hier enttäuscht, dass die DS-GVO kein Konzernprivileg beinhaltete.

Aus datenschutzrechtlicher Sicht ist es jedoch unabdingbar, dass kein Konzernprivileg existieren kann. Schon 1976 wurde bei der Einführung des BDSG über die Aufnahme eines Konzernprivilegs diskutiert, jedoch entschied man sich gegen eine entsprechende Begünstigung von Unternehmensverbünden[1]:

„Es stellte sich ferner die Frage, wie der Datenfluß innerhalb wirtschaftlich verbundener Unternehmen geregelt werden solle. Der Ausschuß entschied sich gegen die Einführung einer entsprechenden Konzernklausel, da andernfalls der Datenschutz in verfassungsrechtlich bedenklicher Weise gerade in wichtigen Bereichen der Wirtschaft eingeschränkt würde. Der betroffene Bürger könnte zwar noch die rechtliche Selbständigkeit eines Unternehmens, nicht aber dessen wirtschaftliche Verflechtungen erkennen. Eine solche Ausnahmeregelung hätte auch zu einer erheblichen Bevorzugung der multinationalen Gesellschaften und andererseits zu einer Benachteiligung der kleineren und mittelständischen Unternehmen geführt“.

Auch im Rahmen der Entwicklung der DS-GVO wurde durch das Europäische Parlament mit Änderungsvorschlag 134 versucht, ein Konzernprivileg einzuführen. Letztlich scheiterte dies mit derselben Begründung, die auch verhinderte, dass in einer der BDSG-Novellen ein Konzernprivileg eingeführt wird: Ein Konzernprivileg verhindert eine Transparenz der Verarbeitung für die betroffene Person, so dass die Person ihre Betroffenenrechte nicht mehr wahrnehmen kann. Daher ist die Einführung eines Konzernprivilegs aus verfassungsrechtlichen Gründen abzulehnen.

Aber auch wenn es ein „echtes“ Konzernprivileg nicht gibt, so gibt es dennoch einige Regelungen, welche eine Konzentrierung der Verarbeitung erleichtern. Einerseits wird in Art. 4 Ziff. 19 DS-GVO der Begriff „Unternehmensgruppe“ als eine „Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht“ definiert. Aus ErwGr. 37 lässt sich entnehmen, dass die vorgenannte Beherrschung weit zu verstehen ist. Um als Unternehmensgruppe zu gelten, ist es entsprechend ErwGr. 37 ausreichend, wenn das herrschende Unternehmen z. B. „aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann“. Somit richtet sich die DS-GVO in einigen Teilen auch direkt an Konzerne.

Gemäß Art. 37 Abs. 2 DS-GVO ist für eine Unternehmensgruppe die Benennung eines gemeinsamen Datenschutzbeauftragten statthaft, d.h. der „Konzerndatenschutzbeauftragte" ist realisierbar und es ist – im Gegensatz zum heutigen BDSG – unter der DS-GVO nicht länger zwingend erforderlich, dass jede Unternehmensgruppe in einem Konzern einen eigenen Datenschutzbeauftragten bestellen muss.

ErwGr. 48, der in der Literatur teilweise als „kleines Konzernprivileg" bezeichnet wird, erleichtert die Übermittlung Personen bezogener Daten in einem Konzern. ErwGr. 48:

„Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln."

Diese Regelung bezieht sich auf Interessenabwägungen bei Beurteilung der Rechtmäßigkeit von Datenverarbeitungen, wie sie sich auch in Art. 6 Abs. 1 S. 1 lit. f DS-GVO wiederfindet. Allerdings muss man hierbei beachten, dass Art. 6 DS-GVO keinen Erlaubnistatbestand zur Verarbeitung besonderer Kategorien von Daten darstellt, deren Verarbeitung ausschließlich durch die in Art. 9 DS-GVO zu findenden Regelungen legitimiert werden kann. Und in Art. 9 DS-GVO ist eine Interessenabwägung in dieser Form nicht vorgesehen. D. h. durch die in ErwGr. 48 in Verbindung mit Art. 6 Abs. 1 S. 1 lit. f DS-GVO erfolgte Normierung des anerkannten Interesses von Unternehmensgruppen an internem Datenaustausch zwecks Verwaltungsoptimierung und -vereinfachung werden Datenflüsse innerhalb einer Konzerngruppe zukünftig leichter zu rechtfertigen sein, jedoch sind davon nicht zwangsläufig besondere Kategorien von Daten erfasst.

Medizinische Versorgung und die DS-GVO

Eine Einschätzung der Auswirkungen der DS-GVO auf die medizinische Versorgung ist schwierig, da derart viele Öffnungsklauseln existieren, dass von einem europaweit geltenden Rechtsrahmen nicht mehr zu sprechen ist. Allerdings enthält die DS-GVO auch einige Regelungen, die abschließend geregelt sind, d.h. eine nationale Abhängigkeit ist nicht gegeben.

Betroffenenrechte

Die Betroffenenrechte entsprechen weitestgehend den heute bekannten Rechten:

- Transparenz (Art. 12 DS-GVO) bei der Verarbeitung ist eine grundlegende Anforderung, damit die informationelle Selbstbestimmung erfolgen kann: Nur wenn die betroffene Person Kenntnis über die Struktur der Datenverarbeitung, die Datenverarbeitungsprozesse, die eingesetzte Technik und die Datenströme besitzt, kann das Recht auf informationelle Selbstbestimmung wahrgenommen werden.
- Information (Artt. 13, 14 DS-GVO) ist ebenfalls aus § 4 BDSG bekannt, jedoch wurden die Informationspflichten erweitert. Zum einen muss die Information regelhaft vor Beginn der Datenverarbeitung erfolgen, zum anderen wurde das Auskunftsrecht erweitert. Neu ist, dass eine Auskunft bzgl. Speicherdauer bzw. – falls dies nicht möglich ist – eine Darlegung der Kriterien für die Festlegung der Speicherdauer zu erfolgen hat.
- Das Recht auf Auskunft (Art. 15 DS-GVO) ist ebenfalls aus § 19 bzw. § 34 BDSG bekannt. Die DS-GVO gibt dabei vor, dass Informationen nur an identifizierte Personen (Betroffene) weitergeben werden dürfen. So soll verhindert werden, dass über ein Auskunftsersuchen unbefugte Personen Zugriff auf personenbezogene Daten erhalten. Neu ist auch die Regelung, dass betroffene Personen bzgl. Zweckänderung zu informieren sind.
- Berichtigung (Art. 16 DS-GVO), Löschung (Art. 17 DS-GVO), Sperrung (Art. 18 DS-GVO) werden auch heute schon von § 6 BDSG gefordert, stellen daher keine Neuerung für deutsche Verarbeiter dar.
- Das Widerspruchsrecht (Art. 21 DS-GVO) findet sich in ähnlicher Form in den §§ 20, 35 BDSG, stellt also ebenfalls keine Neuerung für deutsche Verarbeiter personenbezogener Daten dar.
- Auch die automatisierte Generierung von Einzelentscheidungen einschließlich Profiling (Art. 22 DS-GVO) findet sich im deutschen Recht wider: In § 6a BDSG finden sich vergleichbare Anforderungen.

Allerdings bringt die DS-GVO auch neue Rechte für betroffene Personen mit sich, die in dieser Form bisher nicht existierten:

1) Empfängern, an die Daten weitergegeben wurden, muss gemäß Art. 19 DS-GVO jede Berichtigung, Löschung oder Einschränkung mitgeteilt werden. Wenn man sich die Menge an Arztbriefen vor Augen führt, die von einem mittelgroßen Krankenhaus versandt werden, wird ersichtlich, welcher Aufwand diese Anforderung für die deutsche Gesundheitsversorgung bedeutet.
2) Art. 20 DS-GVO postuliert ein „Recht auf Datenübertragbarkeit". Unter der Voraussetzung, dass die Rechtmäßigkeit der Verarbeitung auf einer Einwilligung oder einem Vertrag gemäß Art. 6 Abs. 1 lit. b beruht, haben betroffene Personen das Recht,
   - Daten „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten" und
   - Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermitteln zu lassen.

Dies bedeutet, dass nahezu jedes auf dem Markt befindliche medizinische Informationssystem angepasst werden muss, damit dieser Anforderung nachgekommen werden kann. Zudem muss festgelegt werden, in welchem Format bzw. in welchen Formaten die Daten ausgetauscht werden. Dies bedeutet Mehrkosten für jede Arztpraxis und jedes Krankenhaus in Deutschland.

Auftragsverarbeitung

Die im Krankenhaus bzw. in der Arztpraxis eingesetzten IT-Systeme werden immer komplexer. Eine Betreuung durch ärztliches Personal ist, unabhängig von allen anderen Gesichtspunkten, schon auf Grund dieser Komplexität nicht möglich. Selbst speziell ausgebildetes IT-Personal des Krankenhauses

bzw. der Arztpraxis ist häufig darauf angewiesen, bei der Betreuung dieser Systeme durch den Hersteller unterstützt zu werden. Eine gewisse Form des Outsourcings der IT-Betreuung ist damit heute unvermeidbar, wenn man nicht die Gefährdung der Patientenbehandlung und ggfs. sogar des Patientenlebens durch nicht funktionierende IT-Systeme auf sich nehmen möchte.

Datenschutzrechtlich erfolgt hier i.d.R. eine Auftragsverarbeitung. Die DS-GVO weist dabei eine nicht so starke technische Ausprägung auf wie das BDSG, sondern ist stärker funktional geprägt. D. h. es steht nicht immer nur die technische Ausprägung eines Auftrags im Vordergrund, wie es beispielsweise bei der Wartung von IT-Systemen der Fall ist, sondern Auftragsverarbeitung kann z. B. auch die Auslagerung von Postdienstleistungen umfassen. Aber es gibt noch mehr Unterschiede.

Unter der aktuellen Rechtslage des BDSG kann eine Auftragsverarbeitung nur im EWR stattfinden, die DS-GVO erlaubt die weltweite Verarbeitung personenbezogener Daten im Auftrag. Dies ist letztliche eine konsequente Abbildung der Realität: die heutige Welt ist stark IT-geprägt, dies gibt selbstverständlich auch für die Gesundheitsversorgung. Dabei kennt letztlich nur der Hersteller der IT-Systeme alle „Geheimnisse", d.h. in letzter Instanz kann auch nur der Hersteller notwendige Funktionen ergänzen oder Fehler in den IT-Systemen beseitigen. Die IT-Systeme werden aber nicht nur von Herstellern aus dem EWR entwickelt, viele kommen aus dem nordamerikanischen Raum. Entsprechend kann eine Auftragsverarbeitung gesetzlich nicht auf den EWR beschränkt werden, die faktische Notwendigkeit bei Bedarf auch eine Auftragsverarbeitung außerhalb des EWR durchführen zu dürfen, ist schlicht vorhanden. Dabei erlaubt die DS-GVO eine Auftragsverarbeitung nur, wenn die von der DS-GVO definierten Rechte betroffener Personen gewahrt bleiben und auch der in der DS-GVO verankerte Schutz der personenbezogenen Daten gewahrt bleibt.

Neu für Deutschland ist ebenfalls, dass dem Auftragsverarbeiter eigenverantwortliche Spielräume für die Umsetzung des Auftrags eingeräumt bekommt; entscheidend für die Auftragsverarbeitung ist, dass der Auftraggeber als Verantwortlicher einen rechtlichen (ggfs. auch einen tatsächlichen) Einfluss auf die Entscheidung bzgl. der Verarbeitung der Daten hat. Im Gegenzug führt die DS-GVO klare Verantwortlichkeiten auch für den Auftragsverarbeiter ein, deren Nicht-Einhaltung eine Aufsichtsbehörde sanktionieren kann. Wie sich dies in Deutschland, wo Aufsichtsbehörden traditionell eher zurückhaltend mit einer Sanktionierung arbeiten, auswirkt, muss abgewartet werden. Verstöße sind europaweit in gleicher Weise zu ahnden, so dass Unternehmen, die in dem einem EU-Land für einen Verstoß härter bestraft werden als Firmen für einen gleichartigen in einem anderen EU-Land eine Klage wegen zu harter Strafen führen können. Die Aufsichtsbehörden müssen sich hier also absprechen und europaweit vergleichbare Strafen einführen.

Sicherheit der Verarbeitung

Gemäß Art. 32 Abs. 1 DS-GVO müssen Verantwortlichen geeignete Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Gesundheitsdaten wie auch genetische Daten, die beide zu den besonderen Kategorien von Daten gehören, erfordern auf jeden Fall ein hohes Schutzniveau. Dabei gibt die DS-GVO vor, dass eine Abwägung bzgl. der zu treffenden technischen und organisatorischen Maßnahmen („TOMs") zur Herstellung eines dem Risiko angemessenen Schutzniveaus zu erfolgen hat. In der Abwägung ist insbesondere zu berücksichtigen:

- Der Stand der Technik
- Die Implementierungskosten
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Der Schutz der Daten ist somit nicht absolut. Z. B. wird eine Arztpraxis ggf. andere Schutzmaßnahmen ergreifen dürfen als ein Krankenhaus, da in der Abwägung die Implementierungskosten für bestimmte Schutzmaßnahmen von beiden Organisationsformen wahrscheinlich unterschiedlich bewertet werden. Die TOMs schließen entsprechend Art. 32 Abs. 1 DS-GVO u.a. Folgendes ein:

- Pseudonymisierung personenbezogener Daten
- Verschlüsselung personenbezogener Daten
- Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten
- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Da die DS-GVO diese Schutzmaßnahmen explizit benennt und Art. 5 DS-GVO eine Rechenschaftspflicht bzgl. des Nachweises der Einhaltung der Anforderungen der DS-GVO einführt, muss jeder Verantwortliche künftig den Nachweis führen, warum eine der genannten Maßnahmen nicht genutzt wurde. Z. B. ist gerade in der medizinischen Versorgung eine Pseudonymisierung nicht immer möglich, künftig muss dies in einer nachvollziehbaren Begründung dokumentiert werden.

Pseudonymisierung

Da Art. 32 Abs. 1 DS-GVO u. a. eine Pseudonymisierung fordert, ist ein Blick darauf, was darunter verstanden wird, sicherlich nicht verkehrt. Art. 4 Abs. 5 DS-GVO definiert Pseudonymisierung als „die Verarbeitung personenbezogener Daten in einer Weise, dass

- die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können,
- wobei diese zusätzlichen Informationen gesondert aufzubewahren sind
- und diese zusätzlichen Informationen TOMs unterliegen,

- die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden."

Allein aus der Begriffsbestimmung lassen sich verschiedene implizit enthaltene Vorgaben ableiten:

1) Pseudonyme Daten stellen gemäß Art. 4 Abs. 1 DS-GVO personenbezogene Daten dar, bei denen eine grundsätzliche Möglichkeit zur Identifikation der Person besteht.
2) Der Vorgang der Pseudonymisierung stellt eine Verarbeitung im Sinne von Art. 4 Abs. 2 DS-GVO dar, somit gelten für eine Pseudonymisierung alle Vorgaben bzgl. der Verarbeitung, insbesondere die Vorgaben von Art. 5 und Art. 6 bzw. Art. 9 DS-GVO.

D. h. auch bei einer Pseudonymisierung muss die Rechtmäßigkeit der Verarbeitung gewährleistet sein. Insbesondere muss bei der Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DS-GVO ein Erlaubnistatbestand zur Pseudonymisierung vorhanden sein.

3) Pseudonyme Daten gelten nur als pseudonym, wenn der die Daten Verarbeitende keine Möglichkeit hat, die Zuordnungsvorschrift zwischen Pseudonym und Personenkennung zu verarbeiten.

Grundsätzlich muss zudem festgehalten werden, dass eine Pseudonymisierung keine Anonymisierungstechnik darstellt, wie die Artikel-29-Datenschutzgruppe in WP 216[2] feststellte: Eine Pseudonymisierung „verringert lediglich die Verknüpfbarkeit eines Datenbestands mit der wahren Identität einer betroffenen Person und stellt somit eine sinnvolle Sicherheitsmaßnahme dar". Insbesondere sind pseudonymisierte Daten nicht mit anonymisierten Informationen gleichzusetzen.

Medizinische Forschung: Unter der DS-GVO überhaupt noch möglich?

Forschung spielt eine zentrale Rolle in der EU, was sich auch im Vertrag über die Arbeitsweise der Europäischen Union widerspiegelt.[3] Auch in der Charta der Grundrechte der Europäischen Union findet sich in Art. 13 die Privilegierung der Forschung wieder[4]: „Kunst und Forschung sind frei". Damit steht die Forschungsfreiheit nur knapp hinter dem Recht auf Schutz personenbezogener Daten, der in Art. 8 der Charta festgehalten ist.

Dieser besonderen Stellung der Forschung trägt auch die DS-GVO Rechnung: Gemäß Art. 5 Abs. 1 lit. b DS-GVO ist eine Änderung des Verarbeitungszweckes für Forschungen grundsätzlich möglich. Natürlich muss die Forschung zur Nutzung der Daten einen Erlaubnistatbestand aufweisen, aber die Möglichkeit der Zweckänderung wäre ohne diese Privilegierung gerade bei Daten der besonderen Kategorien, wozu ja Gesundheitsdaten als auch genetische Daten gehören, gar nicht möglich.

Weiterhin müssen alle Forschungsaktivitäten, bei denen personenbezogene Daten verarbeitet werden, gemäß Art. 89 Abs. 1 DS-GVO im datenschutzrechtlichen Sinne ausgestaltet werden. Dies heißt:

- Beachtung datenschutzrechtlicher Grundsätze, insb. Art. 5 DS-GVO (Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung, Rechenschaftspflicht, …)
- Beachtung der Betroffenenrechte, insbesondere Informationspflichten (Erhebung, Zweckänderung) und Widerspruchsrecht
- Verarbeitung nur bei Vorhandensein „geeigneter" technischer und organisatorischer Maßnahmen (insbesondere Artt. 25, 30, 32 DS-GVO)

Was ist eigentlich „Forschung"?

Der Begriff der „Forschung" selbst ist in der DS-GVO nicht definiert. Die Erwägungsgründe geben aber eine Vorstellung, was der europäische Gesetzgeber darunter versteht, z. B.

- Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden (Erwägungsgründe 53, 159)
- Klinische Prüfungen (Erwägungsgrund 156)
- Register (Erwägungsgrund 157)
- Verbesserung der Lebensqualität zahlreicher Menschen (Erwägungsgrund 157)
- Verbesserung der Effizienz der Sozialdienste (Erwägungsgrund 157)
- Grundlagenforschung (Erwägungsgrund 159)
- Angewandte Forschung (Erwägungsgrund 159)
- Privat finanzierte Forschung (Erwägungsgrund 159).

Daraus abgeleitet kann man Forschung wie folgt definieren:

*„**Forschung** ist die systematische Suche nach neuen Erkenntnissen sowie deren Dokumentation und Veröffentlichung, wobei Suche sowohl im Bereich der Grundlagenforschung als auch der angewandten Forschung erfolgen kann. Die Ergebnisse der Suche müssen darauf abzielen, dass die Erkenntnisse*

a) dem öffentlichen Interesse im Bereich der öffentlichen Gesundheit dienen oder
b) der Verbesserung der Lebensqualität zahlreicher Menschen oder der Verbesserung der Effizienz der Sozialdienste dienen oder
c) der klinischen Prüfung therapeutischer Maßnahmen dienen oder
d) der Registerforschung dienen.

Die privat finanzierte Forschung ist dabei der öffentlichen Forschung gleichgestellt."

Die wissenschaftliche Forschung ist als ein spezieller Bereich der Forschung anzusehen. Im „Hochschul-Urteil[5]" definierte das Bundesverfassungsgericht: „[…] wissenschaftliche Tätigkeit, d. h. auf alles, was nach Inhalt und Form als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist. […]". Gemäß obiger Definition und unter Berücksichtigung des Urteils des BVerfG lässt sich „wissenschaftliche Forschung" daher wie folgt definieren:

*„**Wissenschaftliche Forschung** ist Forschung, die sowohl nach Inhalt als auch der Form entsprechend als ernsthafter planmäßiger Versuch zur Ermittlung der Wahrheit anzusehen ist."*

Dabei lässt sich aus Art. 5 Abs. 3 Grundgesetz wie auch aus Art. 13 der Charta der Grundrechte der Europäischen Union ableiten, dass die Teilnahme am Wissenschaftsbetrieb grundsätzlich nicht an Voraussetzungen oder Bedingungen geknüpft ist, sondern jedermann auch außerhalb des akademischen oder industriellen Wissenschaftsbetriebs offensteht.

Erlaubnis zur Verarbeitung

Die Verarbeitung besonderer Kategorien von Daten zu Forschungszwecken wird in Art. 9 Abs. 2 lit. j DS-GVO geregelt. Dabei gelten folgende Voraussetzungen (siehe auch ErwGr. 156):

- die Verarbeitung erfolgt auf der Grundlage
- des Unionsrechts oder des Rechts eines Mitgliedstaats,
- welches in angemessenem Verhältnis zu dem verfolgten Ziel steht,
- den Wesensgehalt des Rechts auf Datenschutz wahrt und
- angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht […].

Um Forschung zu ermöglichen müssen die Mitgliedstaaten also nationale Regelungen erlassen, welche den Anforderungen der DS-GVO genügen. Im medizinischen Kontext bedeutet dies für Deutschland, dass die nationalen Regelungen wie sie beispielsweise im Arzneimittelgesetz oder dem Medizinprodukterecht zu finden sind, anzupassen sind.

Datensparsamkeit

Grundsätzlich gilt auch für die Forschung die aus Art. 5 Abs. 1 lit. c DS-GVO resultierende Pflicht zur Datenminimierung, die wir noch als die aus § 3a BDSG resultierende Pflicht zur Datensparsamkeit kennen. Grundsätzlich dürfen nur die personenbezogenen Daten verarbeitet werden, deren Verarbeitung zur Erreichung des Zieles erforderlich ist.

In der DS-GVO selbst wird der Begriff der „Erforderlichkeit“ nicht definiert. Allerdings finden sich in den Erwägungsgründen Kriterien, welche die Beurteilung der Erforderlichkeit erleichtern. Die Verarbeitung von Daten ist insbesondere dann erforderlich, wenn

- der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann (Erwägungsgrund 39) oder
- der Zweck der Verarbeitung im lebenswichtigen Interesse der betroffenen Person liegt (Erwägungsgrund 112).

D. h., damit eine Maßnahme erforderlich ist, darf es kein milderes (= in die Rechte Betroffener weniger eingreifendes) Mittel geben, welches den gleichen Erfolg mit vergleichbarem Aufwand erreicht. Um die Erforderlichkeit/Notwendigkeit beurteilen zu können, müssen (nicht nur) Forscher daher drei Fragen beantworten:

1) Gibt es ein anderes Mittel?
2) Ist dieses in gleicher Weise geeignet, den Zweck zu erreichen?
3) Ist dieses Mittel ein milderes, also die Rechte der betroffenen Person weniger belastendes Mittel?

Fazit

Auch wenn sich das grundlegende Prinzip des Datenschutzes nicht änderte, ergeben sich sehr viele Änderungen bei der Verarbeitung personenbezogener Daten. Für Konzerne wie Klinikketten wird die konzerninterne Übermittlung von Beschäftigtendaten zur zentralen Verarbeitung im Vergleich zu heute erleichtert, jedoch sind besondere Kategorien von Beschäftigtendaten wie z. B. Krankmeldungen gesondert zu betrachten. Der damit verbundene Aufwand reduziert die Nützlichkeit die ErwGr. 48, so dass im Vergleich zu heute der Aufwand bei der konzerninternen Verarbeitung von Beschäftigtendaten in etwa gleich bleibt.

Die Auftragsverarbeitung wurde „generalüberholt“. Auch wenn sich in den grundlegenden Anforderungen bzgl. Vertragsgestaltung im Vergleich zu heute wenig änderte, erfolgte doch eine begrüßenswerte Anpassung der Rahmenbedingungen, welche der heute stattfindenden Verarbeitung gerecht wird.

Auch heute schon gehören die bei der Versorgung anfallenden Patientendaten zu den Daten mit dem höchsten Schutzbedarf. Die Nachweispflichten der DS-GVO erhöhen die Dokumentationspflichten enorm. Schon heute wird überall in der Gesundheitsversorgung beklagt, dass der administrative Aufwand zu hoch ist und zu wenig Zeit für den Patienten übrig bleibt; die DS-GVO wird dieses Ungleichgewicht verstärken, auch wenn grundsätzlich die geforderte Rechenschaftspflicht richtig ist.

Schon bei Einführung der EU Datenschutz-Richtlinie 95/46/EG wurde von einigen Autoren das Ende der Forschung in Deutschland postuliert[6], ähnliches konnte man bei der Einführung der DS-GVO sehen. Richtig ist, dass die Forschung mit Patientendaten Schutzmaßnahmen verlangt, welche den Forschungsaufwand erhöhen. Wenn man die Sensibilität dieser Daten bedenkt, kann man die Anforderungen der DS-GVO nur als angemessen bezeichnen. Wenn die Anforderungen steigen, so reagiert der Gesetzgeber damit nur auf die verbesserten Möglichkeiten der automatisierten Datenverarbeitung: Wachsende Möglichkeiten der IT bedingen auch einen wachsenden Schutzbedarf. Wo vor 20 Jahren schon allein die Datenmenge einen ausreichenden Schutz bedeutete, ist dies heute nicht mehr gegeben und daher müssen andere Rahmenbedingungen als vor 20 Jahren gelten. Dies gilt natürlich auch abseits der Forschung. Wie man aber in den letzten 20 Jahren sehen konnte, wurde in Deutschland trotz Geltung der RL 95/46/EG überaus erfolgreich geforscht, so dass man die bzgl. der Regelungen der DS-GVO geäußerten Befürchtungen unter „Sturm im Wasserglas“ einsortieren kann.

Obwohl die deutsche Regierung entsprechend der Darstellung von LobbyPlag[7] am stärksten versuchte, das von der DS-GVO geforderte Datenschutzniveau möglichst verarbeitungsfreundlich zu gestalten, kann man aus heutiger Sicht sagen, dass die DS-GVO trotz deutscher Bemühungen einen angemessenen Weg zwischen dem Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und den Interessen der Gruppen, die diese Daten verarbeiten müssen (wie z. B. Krankenhäuser und Arztpraxen), darstellt.

1 Bericht und Antrag des Innenausschusses (4. Ausschuß) zu dem von der Bundesregierung eingebrachten Entwurf eines Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz — BDSG) - Drucksache 7/1027. Online, zitiert am 2017-08-29; Verfügbar unter http://dipbt.bundestag.de/doc/btd/07/052/0705277.pdf

2 Artikel-29-Datenschutzgruppe: Stellungnahme 5/2014 zu Anonymisierungstechniken. Online, zitiert am 2017-08-29; Verfügbar unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_de.pdf

3 Vgl. Art. 179 Abs. 1 AEUV (Teil XIX „Forschung, technologische Entwicklung und Raumfahrt“): „Die Union hat zum Ziel, ihre wissenschaftlichen und technologischen Grundlagen dadurch zu stärken, dass ein europäischer Raum der Forschung geschaffen wird […]“. Online, zitiert am 2017-08-29; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A12012E%2FTXT

4 Charta der Grundrechte der Europäischen Union. Online, zitiert am 2017-08-29; Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A12012P%2FTXT

5 BVerfG, Urteil vom 29.05.1973, AZ.: 1 BvR 424/71 bzw. 1 BvR 325/72 (Hochschul-Urteil). Online, zitiert 2017-08-28; Verfügbar unter https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BVerfG&Datum=29.05.1973&Aktenzeichen=1%20BvR%20424/71. Kommentierung siehe z. B. Epping/Lenz/Leydecker „Sachlicher Schutzbereich der Wissenschaftsfreiheit“ in Epping. Grundrechte. 6. Auflage 2015, Springer-Verlag, ISBN 978-3-642-54657-0

6 Z. B. Mayen, T. (1997) Die Auswirkungen der Europäischen Datenschutzrichtlinie auf die Forschung in Deutschland. NVwZ: 446-451. „Schon die bestehenden Datenschutzgesetze in Deutschland enthalten wichtige und weitreichende Beschränkungen zu Lasten der wissenschaftlichen Forschung. Diese Beschränkungen erschweren nicht nur die Arbeit der wissenschaftlichen Forschung, sondern machen wegen der Unbestimmtheit und Rechtsunsicherheit der einzelnen Klauseln eine Zusammenarbeit zwischen Forschung und Datenschutzbehörden im Einzelfall notwendig. Diese Anforderungen werden durch die neue Europäische Datenschutzrichtlinie nicht vermindert, sondern in einigen Punkten eher noch verschärft.“

7 LobbyPlag.eu: Thomas De Maizière, Germany auf Platz 1 im negativen Ranking. Online, zitiert 2017-08-28; Verfügbar unter http://lobbyplag.eu/governments

Michael Krawczak, Thilo Weichert

Medizinforscher und Datenschützer fordern Bund-Länder-Staatsvertrag

In einer gemeinsamen Initiative legten der Medizininformatiker Prof. Dr. Michael Krawczak und der Datenschützer Dr. Thilo Weichert, Vorstandsmitglied der DVD und Mitglied im Netzwerk Datenschutzexpertise, einen Vorschlag für die Schaffung einer „modernen Dateninfrastruktur für die medizinische Forschung in Deutschland“ vor. Ziel ihrer Initiative ist es, die unübersichtlichen, teilweise widersprüchlichen und nicht praktikablen Strukturen und Regelungen der Datennutzung in der medizinischen Forschung in Deutschland durch ein klares und einheitliches Verfahren zu ersetzen, das den Anforderungen an den Datenschutz ebenso genügt wie den Erwartungen und Bedürfnissen der Wissenschaft. Dadurch soll das Recht auf informationelle Selbstbestimmung ebenso gestärkt werden wie die Konkurrenzfähigkeit des Medizin- und Wissenschaftsstandorts Deutschland.

Weichert und Krawczak richten an Bund und Länder die Bitte, die Rahmenbedingungen für die Verwendung personenbezogener Daten für die medizinische Forschung über einen Staatsvertrag zu vereinheitlichen. So könnten praktikable Voraussetzungen für Krankheitsregister, Biobanken, Forschungsverbünde und weitere überregionale Projekte entstehen, wie sie derzeit u. a. durch die Medizininformatik-Initiative der Bundesregierung mit 150 Millionen Euro gefördert werden. Grundidee des Vorstoßes von Weichert und Krawczak ist die rechtliche Aufwertung der allenthalben etablierten oder neu entstehenden, sogenannten „Use and Access Committees“ (UAC) von Forschungsverbünden zu Melde- und Genehmigungsstellen. Der Vorschlag knüpft an die europäische Datenschutz-Grundverordnung an, die ab 25.05.2018 direkt anwendbar sein wird. Ein zentrales Anliegen ist dabei die Verbesserung der Forschungstransparenz durch den Betrieb einer Internet-Plattform, auf der gemeldete und genehmigte Medizinforschungsprojekte dargestellt und Außenstehende über deren Fortgang informiert werden. Der Vorschlag entstand in einem umfassenden Dialog mit Medizin- und Forschungseinrichtungen, Datenschützern und Politik.

Thilo Weichert: „Die Hoffnung, dass nach Inkrafttreten der europäischen Datenschutz-Grundverordnung eine Bereinigung der Datenschutzklauseln im Forschungsbereich stattfinden würde, erwies sich bisher als falsch. Insbesondere im sensitiven medizinischen Bereich, wo einrichtungsübergreifend und international gearbeitet werden muss, wird so weiterhin der Datenschutz oft übergangen; wichtige Projekte werden durch bürokratisches Kleinklein behindert. Wir wollen hohe Datenschutzstandards, die aber einfach durch die Forschenden umzusetzen sind. Eine solche Regulierung ist überfällig.“

Michael Krawczak vom Institut für Medizinische Informatik und Statistik der Universität Kiel: „Medizinische Forschung dient durch die Gewinnung neuer wissenschaftlicher Erkenntnisse maßgeblich der besseren Versorgung der Patienten. Um jedoch international konkurrenzfähig zu sein, benötigt die Forschung einheitliche Verfahren und

Standards. Dem stehen die aktuellen Regelungen und Strukturen entgegen. Die Bundesregierung kann diesen Missstand zu Beginn der neuen Legislaturperiode in einer gemeinsamen Anstrengung mit den Ländern abstellen. Wir sind uns sicher, dass Datenschützer und Medizinforscher sie dabei gleichermaßen unterstützen werden. Gerade die aktuelle Medizininformatik-Initiative der Bundesregierung würde von einer solchen Initiative erheblich profitieren und den für einen langfristigen Erfolg notwendigen rechtlichen Rückhalt bekommen".

Vorgeschichte

Die Initiatoren des Vorschlags einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland kennen einander aus ihrer beruflichen Befassung mit dem Thema. Michael Krawczak ist seit über 30 Jahren in den Bereichen Bio- und Medizininformatik sowie Genforschung tätig und hat in Kiel das Biobankenprojekt Popgen mit aufgebaut. Er ist Leiter des Instituts für Medizinische Informatik und Statistik der Christian-Albrechts-Universität zu Kiel. Thilo Weichert war viele Jahre in der Datenschutzaufsicht tätig und leitete von 2004 bis 2015 die schleswig-holsteinische Datenschutzaufsichtsbehörde, das Unabhängige Landeszentrum für Datenschutz in Kiel. Beide Initiatoren stellten – jeweils aus ihrem Blickwinkel – fest, dass beim Datenschutz in der medizinischen Forschung vieles im Argen liegt. Dies sei weder bösem Willen noch mangelnder Dialogbereitschaft von Datenschützern und Medizinforschern zuzuschreiben, sondern überholten rechtlichen Regelungen und einer unzureichenden organisatorischen Infrastruktur.

Dies veranlasste Krawczak und Weichert, Ende 2016 eine gemeinsame Initiative zu starten mit dem Ziel, eindringlich auf die bekannten Missstände hinzuweisen und so einen Beitrag zu deren Behebung zu leisten. Sie erarbeiteten gemeinsam ein Thesenpapier, das einigen ausgewählten ExpertInnen zur Kommentierung zuging. Daraus entstand ein Textentwurf, der am 10.07.2017 an über 50 einschlägige Adressen versandt wurde mit der Bitte um kritische Kommentierung. Adressaten waren u. a. die zuständigen Bundesministerien, die Bundestagsfraktionen, im Medizinbereich tätige Forschungseinrichtungen und -verbände, Datenschutzbeauftragte sowie Datenschutz- und Verbraucherschutzorganisationen.

Die Autoren erhielten eine Vielzahl schriftlicher, elektronischer, mündlicher und telefonischer Rückmeldungen. Am 20.07.2017 in Berlin wurden die Vorschläge im Rahmen des Workshops „Datenschutz in der medizinischen Forschung" der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (gmds) diskutiert.

Reaktionen aus der Politik

Aus dem Bundestag antworteten die Fraktionen von CDU/CSU, SPD und Bündnis 90/Die Grünen. Die positivste Reaktion kam von den Grünen, die den Vorschlag einer Verringerung der rechtlichen Zersplitterung als interessant und unterstützungswert beurteilten. Die Möglichkeiten der Nutzung von Daten für die Versorgungsforschung müsse im Rahmen der schützenden Vorgaben der EU-DSGVO verbessert, die Bearbeitungszeiten von Forschungsanträgen verkürzt und aktuelle Datenbeständen besser verfügbar gemacht werden. Die CDU/CSU-Fraktion bestätigte die Notwendigkeit, politisch tätig zu werden, und verwies auf eigene programmatische Äußerungen. Die SPD-Fraktion teilte mit, dass die Vorschläge der Initiatoren von den Gremien „bei der weiteren politischen Arbeit" berücksichtigt würden.

Wissenschaftsgesellschaften

Der Rat für Informationsstrukturen (RfII), der im März 2017 Empfehlungen zu Datenschutz und Forschungsdaten mit vergleichbarer Zielrichtung veröffentlicht hatte[1], signalisierte seine grundsätzliche Unterstützung der Vorschläge.

Der Wissenschaftsrat (WR) teilte mit, dass er unlängst eine Arbeitsgruppe zu den „Rahmenbedingungen datenintensiver Wissenschaft" eingerichtet hat; Dateninfrastrukturen für die medizinische Forschung seien seit Längerem ein wichtiges Thema für den WR. Das Deutsche Netzwerk Versorgungsforschung (DNVF) schloss sich den von den Initiatoren dargelegten Einschätzungen und Vorschlägen an.

Die Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (gmds) verwies darauf, dass sie im Frühjahr 2017 gemeinsam mit anderen Fachgesellschaften (AWMF, BVMI, bvitg, DGepi, IBS und GI) ein „Memorandum zum Datenschutz in der medizinischen Forschung" mit ähnlicher Zielrichtung veröffentlicht hat.[2] Eine ausführliche Stellungnahme gab der gemeinsame Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen" der gmds und der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) ab. Darin wurde der Vorstoß der Initiatoren generell begrüßt und es wurde auf parallele Bestrebungen hingewiesen. Die Stellungnahme enthielt u. a. Kommentare zum Verzicht auf Einwilligungen bei „unverhältnismäßigem Aufwand", zum Patientengeheimnis und zu einem möglichen Forschungsgeheimnis, zum Vorrang der Anonymisierung sowie zur Rolle der Ethik-Kommissionen. Hinsichtlich des weiteren Vorgehens wurde angeregt, die bisherigen Initiativen zu verknüpfen und die Bundesländer, insbesondere mit Blick auf die notwendige Anpassung der aktuellen Gesetzeslage an die DSGVO, stärker einzubeziehen.

Weitere Institutionen

Die Landesbeauftragte für den Datenschutz Niedersachsen sieht als Vorsitzende der Konferenz der Datenschutzbehörden in den von den Initiatoren gemachten Vorschlägen „eine gute Grundlage für eine Erörterung eventueller Optimierungsmöglichkeiten der bestehenden bundes- und landesrechtlichen Forschungsklauseln" und kündigte an, auf eine vertiefte Befassung durch die Gremien der Datenschutzaufsichtsbehörden hinzuwirken. Auch das Bundesministerium für Gesundheit sowie der Digitalverband Bitkom kündigten an, sich mit den Vorschlägen der Initiatoren weiter zu befassen.

Änderungen des Vorschlags

Auf der Grundlage der Rückmeldungen wurden die Vorschläge wie folgt verändert: Es wurde präzisiert, dass sich

die Vorschläge nicht auf die medizinische Forschung im Allgemeinen und insbesondere nicht auf die Direkterhebung von Daten für Forschungszwecke beziehen, sondern zunächst ausschließlich auf die Zweitnutzung, also die Weiterverwendung existierender medizinischer Daten für Forschungszwecke. Hinsichtlich der direkten Datenerhebung soll vorläufig an den existierenden Regeln und insbesondere an der Einbindung der Ethik-Kommissionen festgehalten werden.

Der Vorschlag eines Bund-Länder-Forschungsgremiums wurde zugunsten eines dezentraleren Ansatzes aufgegeben: Anstelle der Melde- und Genehmigungspflicht gegenüber einer zentralisierten Instanz sollen bestehende, aber bisher rechtlich nicht abgesicherte Instrumente normiert und verbindlich zum Einsatz gebracht werden. Viele größere Forschungsprojekte verfügen schon heute über so genannte „Use-and-Access-Committees“ (UAC), die für die Compliance und Fachlichkeit des Umgangs mit medizinischen Forschungsdaten zuständig sind. Derartige UAC sollten künftig an allen Einrichtungen etabliert werden, die in nennenswertem Umfang medizinische Forschung betreiben. Komplexere Forschungsprojekte müssten nachweisen, dass sie ein Melde- bzw. Genehmigungsverfahren eines dieser UAC durchlaufen haben. Um die Unabhängigkeit und interdisziplinäre Fachlichkeit der UAC sicherzustellen, werden sie gemäß normativ festgelegten Regeln zertifiziert. Die im vorherigen Vorschlag formulierten Anforderungen an das Bund-Länder-Forschungsgremium hinsichtlich Qualität, Prozessen und Transparenz sind in gleicher Weise an die UAC zu stellen. Für die Kommunikation zwischen den zertifizierten UAC und der (Fach-) Öffentlichkeit ist eine geeignete informationelle Infrastruktur normativ vorzugeben und zu schaffen.

Als normative Grundlage wird weiterhin ein Bund-Länder-Staatsvertrag vorgeschlagen. Dem Bund und den Bundesländern bleibt es aber unbenommen, für die medizinische Forschung bis zur Einigung über einen derartigen Staatsvertrag in den jeweiligen Zuständigkeitsbereichen die organisatorischen und normativen Grundlagen vorwegzunehmen. Zugleich sollten in der EU vergleichbare und ergänzende Anstrengungen angeregt werden.

Mittelfristig wird nicht ausgeschlossen, dass die auf den UAC basierende Forschungsinfrastruktur – wie zunächst vorgeschlagen – in Richtung einer Bund-Länder-Einrichtung weiterentwickelt wird.

Die gegenüber dem ersten Vorschlag vorgenommenen Änderungen haben folgende Vorteile: Es kann an bestehende und im Rahmen des „Förderkonzepts Medizininformatik“ des Bundesforschungsministeriums ohnehin notwendige organisatorische Maßnahmen angeknüpft und diesen zugleich eine höhere Verbindlichkeit verliehen werden. Die Notwendigkeit der Etablierung einer Bund-Länder-Mischverwaltung mit den damit verbundenen Legitimations- und Kontrollproblemen kann vorläufig zurückgestellt werden. Zurückgestellt werden kann damit auch der mit einem zentralen Gremium verbundene personelle und organisatorische Aufwand. Die bisherigen Zuständigkeiten in den Bereichen Medizinethik und Datenschutz können vollständig erhalten bleiben und werden lediglich durch die UAC ergänzt. Bisher praktizierte Abläufe, die sich als aufwändig und ineffektiv erwiesen haben, werden aufgegeben.

Die im Folgenden abgedruckten Vorschläge der Initiatoren sowie deren Begründung sind auch im Netz zu finden unter http://www.uni-kiel.de/medinfo/documents/TWMK%20Vorschlag%20DInfMedForsch%20v1.9%20170927.pdf.

Vorschlag einer modernen Dateninfrastruktur für die medizinische Forschung in Deutschland

1. Hintergrund

Gesundheitsdaten fallen nicht nur im Krankenhaus und in der Arztpraxis an. Vielmehr werden medizinische Leistungen heute auch in großem Umfang durch nichtärztliche Heilberufe erbracht, von Psychologen und Apothekern bis zu Heil- und Pflegediensten. Diese nehmen für die finanzielle, organisatorische und informationstechnische Unterstützung ihrer Aktivitäten selbst wieder Dienstleister in Anspruch, so dass Gesundheitsdaten in einer Vielzahl öffentlicher und geschlossener Netze, Rechenzentren und Serviceeinrichtungen auftauchen. Systembedingt müssen auch kassenärztliche Vereinigungen, Krankenkassen und Medizinischer Dienst sowie private Abrechnungsprüfer und Versicherungen personenbezogene medizinische Daten verarbeiten. Und nicht zuletzt erzeugen Menschen auch immer öfter durch Eigenerhebung mittels sog. Wearables gesundheitsrelevante Daten, die dann in sozialen Netzwerken oder bei Internet-Dienstleistern gespeichert und getauscht werden. Gleiches gilt für die Nutzung internetgestützter Beratungsdienste, Selbsthilfeportale und Suchmaschinen.[3]

2 Chancen und Risiken

Die rasante Verbreitung digitaler Gesundheitsdaten bedeutet zugleich Herausforderung und Chance für die medizinische Forschung. Sie verspricht zweifellos einen immer **reichhaltigeren Erkenntnisgewinn** mit der Aussicht auf neue diagnostische und therapeutische Möglichkeiten. Besonders im Bereich der Bio-, speziell der Gentechnik, tun sich gänzlich neue Zugänge zu Erkrankungs- und Therapiemechanismen auf.[4] Diesen Chancen stehen jedoch auch Risiken für die Beteiligten gegenüber. Bei **Verletzung der Vertraulichkeit** besteht die Gefahr, dass sich Patienten gegenüber den sie behandelnden Ärzten nicht mehr hinreichend öffnen, was wiederum eine umfassende und wirkungsvolle medizinische Hilfe erschwert. Diese Erkenntnis fand schon vor über 2000 Jahren Eingang in den Eid des Hippokrates und behielt – eingebettet in medizinisches Standesrecht und Sanktionsregelungen wie den § 203 StGB – bis heute ihre Gültigkeit. Reichhaltige und weithin verfügbare Gesundheitsdaten bergen zudem die Gefahr einer **medizinisch begründeten Diskriminierung**, etwa beim Versicherungsschutz oder bei der konkreten Behandlung, auch wenn dies oftmals aus fachlichen Gründen unsinnig ist. Und nicht zuletzt bieten Gesundheitsdaten ein weites Feld für das Verfolgen **kommerzieller Interessen** – von der gezielten Produktwerbung bis zum expliziten Handel mit Daten.

3 Rechtlicher Rahmen

Angesichts der dargestellten Dynamik gilt es, in Deutschland rechtliche und infrastrukturelle Voraussetzungen für eine wissenschaftliche Nutzung von Gesundheitsdaten zu schaffen, die Forscher die verfügbaren technischen Möglichkeiten ausschöpfen und zugleich die damit verbundenen Risiken beherrschen lässt. Richtschnur dieser Entwicklung muss zweifellos der bestehende **verfassungsrechtliche Rahmen** sein, der den Schutz der Gesundheit (Art. 2 Abs. 2 GG, Art. 3, 35 GRCh) und das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG, Art. 8 GRCh) verspricht, gleichzeitig aber die Berufsfreiheit medizinischer Leistungserbringer (Art. 12 GG, Art. 15 GRCh) und die Wissenschaftsfreiheit (Art. 5 Abs. 3 GG, Art. 13 GRCh) garantiert.

Bereits heute gibt es einen europaweit einheitlichen Rahmen für die Datenschutzgesetzgebung. Umso mehr verblüfft, wie fragmentiert und antiquiert die **einfachgesetzlichen Regeln** zur Nutzung von Gesundheitsdaten für Forschungszwecke auf nationaler Ebene immer noch sind. In Deutschland finden sich entsprechende Regelungen in den allgemeinen Datenschutzgesetzen des Bundes und der Länder (vgl. §§ 40, 28 Abs. 6 Nr. 4, 14 Abs. 2 Nr. 9, 4a Abs. 3 BDSG-alt, § 22 LDSG SH), die auf die Spezifik von Gesundheitsdaten als besonders sensitive Kategorie (vgl. § 3 Abs. 9 BDSG-alt) jedoch nur bedingt eingehen. Die ohnehin verstreuten allgemeinen Forschungsklauseln werden durch spezifische Regelungen in Spezialgesetzen ergänzt, was die Rechtslage unüberschaubar und ihre praktische Umsetzung schwierig macht.[5] Teilweise wird

- externe Forschung gar nicht oder nur anderen Fachabteilungen derselben juristischen Person erlaubt,
- der Einsatz externen Personals vor Ort vorausgesetzt,
- die Datennutzung auf das jeweilige konkrete Forschungsprojekt beschränkt,
- die Formulierung von Aufklärung und Einwilligung spezifischen Anforderungen unterworfen,
- die Nutzung für andere Projekte an eine umfassende Anonymisierung geknüpft, oder
- die Einbeziehung von Datenschutzbehörden oder anderen Stellen gefordert.[6]

Das bestehende Regelungschaos könnte nun Dank europäischer Vorgaben beseitigt werden.[7] Mit der im Mai 2016 in Kraft getretenen und zwei Jahre später direkt anwendbaren **Europäischen Datenschutzgrundverordnung** (DSGVO) wurde ein supranationaler Rechtsrahmen geschaffen, in dem Gesundheitsdaten (Art. 4 Nr. 15 DSGVO) weiterhin einen hohen Schutz genießen (Art. 9 DSGVO), deren Weiterverarbeitung zu Forschungszwecken aber als von hohem öffentlichem Interesse und nicht länger unvereinbar mit dem ursprünglichen Erhebungszweck eingestuft wird (Art. 5 Abs. 1 lit. b DSGVO). Eine wissenschaftliche Verarbeitung personenbezogener Gesundheitsdaten soll demnach zulässig sein, wenn „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person" vorgesehen sind (Art. 9 Abs. 2 lit. j, 89 DSGVO).[8] Leider wird die so gehegte Hoffnung auf eine Vereinheitlichung und Modernisierung der Datenschutzregelungen zur medizinischen Forschung dadurch getrübt, dass Öffnungsklauseln die Konkretisierung der „Maßnahmen" den nationalen Gesetzgebern überlassen und die (nationalen) Regelungen zum Berufsgeheimnisschutz unberührt bleiben (Art. 9 Abs. 3 u. 4, 90 DSGVO).

Im schlimmsten Fall kann also alles beim Alten bleiben. Das im April 2017 vom deutschen Bundestag beschlossene **Bundesdatenschutzgesetz** (BDSG-neu) enthält zwar in § 27 Abs. 1 die Erlaubnis zur Verarbeitung sensitiver Daten für Forschungszwecke, wenn

- „die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen" (Satz 1) und
- „angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person" (Satz 2) gemäß § 22 Abs. 2 S. 2 BDSG-neu ergriffen werden.

Allerdings ist laut § 27 Abs. 3 BDSG-neu auch weiterhin eine frühestmögliche Anonymisierung gefordert, und Merkmale, „mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können", sind bis zur Anonymisierung gesondert zu speichern.

Das BDSG-neu schafft **weder Rechtssicherheit noch Rechtsklarheit**, da der gesamte Flickenteppich von Regelungen zur Forschungsdatenverarbeitung, die als bereichsspezifisches Recht vorrangig anzuwenden sind, fortbesteht.[9] Gemäß Art. 9 Abs. 3 DSGVO bleibt zudem das nationale Recht zu Berufsgeheimnissen erhalten, was getreu dem in Deutschland bestehenden Zwei-Schranken-Prinzip bedeutet, dass die Weiterverarbeitung von Berufsgeheimnissen (wie etwa des Patientengeheimnisses) durch Dritte neben der datenschutzrechtlichen Erlaubnis eine zusätzliche Offenbarungsbefugnis verlangt.[10] Die völlig offen formulierte Regelung in § 27 BDSG-neu kann diesbezüglich nicht zufriedenstellen.

Mit diesem leidigen Sachstand ist jedoch die gute Botschaft verbunden, dass der **Gesetzgeber in Deutschland** wegen DSGVO und § 27 BDSG-neu erneut tätig werden muss, wenn Berufsgeheimnisse künftig überhaupt noch für Forschungszwecke genutzt werden sollen. Im Zuge dessen gehören unseres Erachtens sämtliche datenschutzrechtliche Forschungsregelungen auf den Prüfstand. Eine solche Bestandsaufnahme würde dem Gesetzgeber die Gelegenheit geben, nicht nur die datenschutzrechtlichen Forschungsregelungen mit dem Berufsgeheimnisschutz in Einklang zu bringen, sondern darüber hinaus für das seit langem angemahnte einheitliche Rechtsregime im Forschungsbereich zu sorgen.[11] Entsprechende Forderungen kommen inzwischen übrigens nicht nur von den Forschenden, sondern auch von Datenschützern.[12]

4 Regulatorische Unzulänglichkeiten

Medizinische Forschung basiert zunehmend auf einrichtungs- und länderübergreifenden Kooperationen, die den Austausch personenbezogener Daten erfordern. Für die betreffenden Datenquellen gibt es in der Regel bereichsspezifische Vorgaben, die die Datennutzung

bzw. -weitergabe an eine Genehmigung oder zumindest Kenntnisnahme durch Ministerien, Ethik-Kommissionen oder Datenschutzbehörden knüpfen. Die daraus resultierenden administrativen Anforderungen bedeuten einen hohen Aufwand für die Forscher und führen wegen rechtlicher Unwägbarkeiten leicht zu Verunsicherungen. Bisweilen können sich einschlägige Regelungen auf unterschiedlichen Ebenen sogar widersprechen (z. B. bei Forschungsprojekten, für die zugleich Bundes- und Landesgesetze anwendbar sind), was Forscher schlimmstenfalls der Gefahr aussetzt, unabsichtlich und unwissentlich gegen rechtliche Vorgaben zu verstoßen.

Über die Erfüllung der datenschutzrechtlichen Vorgaben hinaus müssen bei vielen medizinischen Forschungsvorhaben analog § 15 MBOÄ auch **Ethik-Kommissionen** einbezogen werden. Dauer und Ergebnis der damit verbundenen Beratungs- und Genehmigungsprozesse sind oftmals schwer einschätzbar.[13] Außerdem kommt es in vielen Belangen zur Doppelung von Aufgaben und Infrastrukturen, da ethische und datenschutzrechtliche Erwägungen teilweise identische Schutzziele verfolgen (Würdeschutz, Persönlichkeitsschutz, sonstiger Grundrechtsschutz). Beide Verfahren fordern letztlich eine Abwägung zwischen Forschungsinteressen und Betroffeneninteressen; sie unterscheiden sich lediglich in der Zusammensetzung des „Spruchkörpers“ und der dort präsenten Expertise.

Sämtlichen Regelungen zur (medizinischen) Forschung ist gemein, dass eine Datennutzung ohne **Einwilligung der Betroffenen** nur im Ausnahmefall und auf der Grundlage einer Güterabwägung erlaubt ist. Vorrang hat die Legitimation durch eine Einwilligung. Dieser Grundsatz folgt dem Wunsch, dass der Betroffene idealerweise selbst bestimmen soll, wer worüber mit seinen Daten forschen darf. Dieses Kernprinzip der informationellen Selbstbestimmung[14] ist unbestritten. Allerdings kann es nicht in allen Lebensbereichen uneingeschränkt realisiert werden, weil Zivilgesellschaften stets eine Balance zwischen individuellen und gemeinschaftlichen Belangen zu wahren haben. Im **überwiegenden Allgemeininteresse** müssen Abweichungen zulässig sein, wobei es allerdings (gesetzlicher) Regeln bedarf, die die Wahrung der Verhältnismäßigkeit garantieren. Insofern sind im Zuge einer Neuregulierung der Nutzung medizinischer Daten für Forschungszwecke organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, die einer Verletzung von Persönlichkeitsrechten effektiv vorbeugen.[15]

Eine wirksame Einwilligung bzw. Schweigepflichtentbindung setzt voraus, dass sie informiert erfolgt, d. h. auf hinreichend präzisen Informationen darüber basiert, welche Stelle für welche Zwecke mit welchen Daten forschen können soll. Aus den nachstehenden Gründen fehlt eine solche klare Information aber oftmals.

- Medizinische Daten bilden ebenso wie Biomaterialien eine dauerhafte Erkenntnisquelle für die Forschung, die nur selten ihren wissenschaftlichen Wert vollends verliert. Viele wissenschaftliche Fragestellungen, die sich mit Daten und Biomaterial bearbeiten lassen, sind zum Erhebungs- bzw. Gewinnungszeitpunkt noch gar nicht genau bekannt. Zudem können sich im Laufe der Forschungsarbeiten neue Fragestellungen ergeben, die ursprünglich ebenso wenig absehbar waren wie die Identität der Einrichtungen, die für die Bearbeitung dieser Fragestellungen am besten qualifiziert und geeignet wären.
- Wegen der Unbestimmtheit der angestrebten Datenverarbeitung werden im Kontext der medizinischen Forschung zunehmend Einwilligungen erbeten, die sehr **umfassend und allgemein formuliert** sind. Daher werden wiederholt Zweifel laut, ob derartige Einwilligungen (sog. broad consent)[16] noch als „informiert“ gelten können und die Funktion einer wirksamen Erlaubnis zur Verarbeitung persönlicher Daten erfüllen. Dies gilt insbesondere für Einwilligungen, die sich in ihrer Unbestimmtheit auch auf ethische „Randzonen“ (z.B. militärische Forschung) erstrecken könnten.
- Die Unbestimmtheit des Verarbeitungszwecks kann teilweise dadurch kompensiert werden, dass die Betroffenen während der Nutzung ihrer Daten regelmäßig oder auf Nachfrage über **aktuelle und geplante Forschungsprojekte** informiert werden (dynamic consent).[17] Dieses Vorgehen ist jedoch oft nicht umsetzbar, z. B. wenn sich die Erreichbarkeit der Betroffenen ändert, die Mitteilung der Informationen das Recht auf Nichtwissen der Betroffenen verletzt, oder ein laufender Kontakt mit Forschenden entweder zu aufwändig oder aus fachlicher Sicht abträglich ist. Diese Unzulänglichkeiten lassen sich teilweise dadurch ausgleichen, dass statt des Einzelnen die Öffentlichkeit als Ganzes informiert wird, oder die Spender ihr Widerrufsrecht für spezielle Forschungsfragen geltend machen.
- Werden Forschungsdaten anonymisiert, so entfallen die Notwendigkeit und die Möglichkeit einer informationellen Selbstbestimmung. Eine Löschung des Personenbezugs steht aber in vielen Fällen den Forschungsinteressen entgegen, da z. B. Langzeitstudien eine fortlaufende Zuordnung neuer Daten zu bereits vorhandenen Daten erfordern. **Langzeitstudien** sind für die medizinische Forschung unerlässlich, da die Wirksamkeit von Therapien und Umweltfaktoren oft erst nach Jahren feststeht.[18]
- Bei Biomaterialien und genetischen Daten besteht wegen der darin enthaltenen Erbinformation ein inhärenter Personenbezug. Ihre unumkehrbare **Anonymisierung ist daher unmöglich**. Allerdings lassen sich die persönlichkeitsrechtlichen Risiken beim Umgang mit genetischen Daten durch den geschickten Einsatz von Pseudonymen und durch die abgeschottete und kontrollierte Verarbeitung der Daten maßgeblich reduzieren.
- Häufig lässt sich das wissenschaftliche Potenzial von Gesundheitsdaten nur durch eine einrichtungsübergreifende (möglicherweise weltweite) **Zusammenführung der Daten** angemessen ausschöpfen, insbesondere bei der Erforschung seltener Erkrankungen. Eine solche Zusammenführung ist bereits heute leicht über Forschungsnetzwerke oder Krankheitsregister realisierbar. Allerdings gibt es hierfür, abgesehen vom Spezialfall der Krebsregistergesetze, keine explizite gesetzliche Grundlage. Die Rechtmäßigkeit der Datennutzung gründet vielmehr allein auf der informierten Einwilligung der Betroffenen mit dem

Vorbehalt, dass Art und Umfang der Datenzusammenführung zum Zeitpunkt der Einwilligung meist völlig unbekannt sind.

In der **weltweiten Diskussion** über die ethischen Anforderungen an medizinische Daten- und Biomaterialbanken hat sich ein weitgehender Konsens entwickelt, der in der Deklaration von Taipeh der World Medical Association (WMA) vom Oktober 2016 festgehalten wurde.[19] Die darin enthaltenen Grundsätze werden vom Standing Committee of European Doctors (CPME) insbesondere mit Blick auf die neuen normativen Herausforderungen durch die DSGVO unterstützt.[20] In Deutschland ist die Rechtssituation der medizinischen Forschung jedoch nach wie vor **praxisfern und fortschrittshemmend**, und es hat bislang keine gesetzgeberischen Versuche gegeben, diese unbefriedigende Situation zu verbessern.

5 Grundsätzliche Überlegungen

Im Folgenden sollen **Regelungsvorschläge** gemacht werden mit dem Ziel, den Vertraulichkeits- und Persönlichkeitsschutz von Patienten und Probanden in der medizinischen Forschung zu gewährleisten und gleichzeitig sicherzustellen, dass das wissenschaftliche Potenzial existierender Datenbestände so weit wie möglich ausgeschöpft wird. Dabei sind folgende **grundsätzliche Erwägungen** anzustellen:

- Moderne Forschungsansätze zielen immer häufiger darauf ab, räumlich und zeitlich auseinanderliegende Datenquellen unterschiedlicher Zweckbindung für eine gemeinsame Analyse zusammenzuführen.
- Zur Sicherung der guten wissenschaftlichen Praxis müssen Forschungsergebnisse unabhängig nachvollziehbar sein, was wiederum die Aufbewahrung der diesen Ergebnissen zugrunde liegenden Daten in möglichst unverändertem Zustand voraussetzt.
- Angesichts der dynamischen Entwicklung von Erzeugung, Erfassung und Auswertung medizinischer Forschungsdaten sind die faktischen Möglichkeiten einer Anonymisierung zunehmend begrenzt.
- Es bestehen heute technische Möglichkeiten (asymmetrische Kryptografie, homomorphe Verschlüsselung), um die Verarbeitung von Forschungsdaten auf bestimmte Stellen und Zwecke zu begrenzen.

Die in Abschnitt 3 thematisierte **Rechtszersplitterung** in Deutschland sollte zugunsten eines möglichst einheitlichen Regelungsregimes beendet werden, das eine gestaffelte Melde- und Genehmigungspflicht für die Verarbeitung personenbezogener Forschungsdaten vorsieht und dadurch in „unkritischen“ Bereichen die Einwilligung der Betroffenen als erforderliche Rechtsgrundlage ersetzt.[21] Allerdings folgt die **Gesetzgebungsbefugnis** im Bereich der Forschung den jeweils zu regelnden Rechtsbereichen und den Zuständigkeiten für die tätigen Einrichtungen. Sie liegt daher sowohl beim Bund als auch bei den Ländern. Ohne Änderung dieser im Grundgesetz festgeschriebenen geteilten Gesetzgebungskompetenzen kann eine einheitliche Regulierung nur durch einen Bund-Länder-Staatsvertrag erfolgen.

Bei der Schaffung einer einheitlichen materiellen Regelung der Datennutzung für die medizinische Forschung sollte auf die Grundsätze **bestehender Forschungsklauseln** zurückgegriffen werden, die sich in der Vergangenheit weitgehend bewährt haben.

- Soweit möglich sind Daten für Forschungszwecke zu anonymisieren; ansonsten ist eine Pseudonymisierung vorzunehmen.[22]
- Eine Verarbeitung personenbeziehbarer Forschungsdaten ist nur zulässig, wenn alle einschlägigen Schutzziele (Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Nichtverkettbarkeit) in angemessener Weise durch technisch-organisatorische Maßnahmen gewährleistet werden.[23]
- Eine Verarbeitung ist zulässig, wenn sie auf einer ausdrücklichen, informierten, freiwilligen und widerrufbaren Einwilligung basiert.[24] Die in der DSGVO (Art 7, 8) enthaltene Regelung würde diesbezüglich auch eine allgemein gültige Präzisierungen für die medizinische Forschung erlauben.
- Eine Verarbeitung kann auch ohne Einwilligung der Betroffenen zulässig sein, wenn das öffentliche Interesse am jeweiligen Forschungsvorhaben die schutzwürdigen Belange der Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.[25]
- Personenbezogene Daten dürfen nur veröffentlicht werden, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung der Forschungsergebnisse unerlässlich ist.[26]
- Die datenschutzrechtlichen Betroffenenrechte müssen stets so weit wie möglich gewährleistet werden.[27]

Forschung mit Berufsgeheimnissen, also insbesondere mit Patientengeheimnissen, erfordert wegen des **Zwei-Schranken-Prinzips**[28] in Deutschland neben der Beachtung allgemeiner Datenschutzregelungen auch die Einhaltung der rechtlichen Anforderungen an die Verarbeitung von Berufsgeheimnissen. Für die arbeitsteilige medizinische Forschung hat dies zur Folge, dass sämtliche Personen, denen Patientengeheimnisse offenbart werden, arbeitsrechtlich der ärztlichen Leitung der Forschungseinrichtung unterstellt werden müssten.[29] Da dies faktisch oft nicht möglich ist, sehen Aufsichtsbehörden in solchen Fällen contra legem über das Fehlen von Offenbarungsbefugnissen hinweg oder interpretieren eine Offenbarungsbefugnis in die allgemeinen Forschungsklauseln hinein.[30] Diese unbefriedigende Rechtslage sollte dahingehend geändert werden, dass an der Forschung Beteiligte unter bestimmten Bedingungen dem Berufsgeheimnis nach § 203 StGB unterworfen werden. Als formaler Ausdruck einer derartigen Auflage sind Genehmigungen oder Zertifikate denkbar.[31]

6 Lösungsvorschlag

Neben technisch-organisatorischen und rechtlichen Regelungen gibt es in den bestehenden Forschungsklauseln auch **prozedurale Vorkehrungen** wie z. B. Genehmigungsvorbehalte und Meldepflichten.[32] Diese haben sich in der Praxis kaum bewährt, weil der Prüfaufwand der beteiligten Stellen (Ethik-Kommissionen, Ministerien, Datenschutzaufsichtsbehörden) mit den vorhandenen Ressourcen nicht erbracht werden konnte. Zudem fehlen diesen Stellen manchmal

das notwendige Problembewusstsein und die nötige Sachkompetenz, was nicht selten zu widersprüchlichen Voten und Entscheidungen geführt hat.

Im Interesse der Entbürokratisierung und Vereinfachung regen wir daher ein Verfahren an, in das technisch-organisatorische, datenschutzrechtliche, ethische und fachliche Erwägungen einfließen können, indem die erforderliche Expertise in **unabhängigen, lokal agierenden Gremien (englisch: Use and Access Committees, UAC)** gebündelt wird.[33] Diesen UACs werden in Abhängigkeit von der Sensitivität des jeweiligen Forschungsvorhabens Genehmigungs- bzw. Vetorechte für die Nutzung personenbezogener Gesundheitsdaten per Gesetz übertragen, erhalten also eine hoheitliche Funktion. In den UACs müssen fachlicher, ethischer und datenschutzrechtlicher Sachverstand vertreten sein. Das Verhältnis der UACs zu den Ethik-Kommissionen und Datenschutzaufsichtsbehörden sollte unter Einräumung eines gegenseitigen Konsultationsrechts so geregelt werden, dass eine Kollision ihrer datenschutz- und berufsrechtlichen Compliance-, Kontroll- und Beratungspflichten weitestgehend vermieden und eine spürbare Entlastung aller Beteiligten erreicht wird. Die Zuständigkeit eines UAC für ein bestimmtes Forschungsprojekt könnte sich aus der geographischen oder organisatorischen Zugehörigkeit des jeweils Projektverantwortlichen ergeben. Vorbild hierfür könnte die in der DSGVO verankerte Regelung zur Zuständigkeit der Aufsichtsbehörden sein, die sich an der Hauptniederlassung eines Verantwortlichen orientiert (Art. 56 Abs. 1).

Während die **organisatorischen und administrativen Verfahren der UACs** gesetzlich zu regeln sind, sollten die Kriterien für die Bewertung von Forschungsvorhaben im Rahmen einer „regulierten Selbstregulierung“ durch Einrichtungen wie z.B. die Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF) entwickelt werden. Die resultierenden Standards könnten im Konsens der betroffenen Fach-Communities auch als verbindlicher und ggf. sogar rechtssicherer Rahmen für die Konzipierung und Zulassung von Forschungsvorhaben dienen.[34]

Derzeit gibt es im Kontext der personenbezogenen Verarbeitung von Daten für medizinische Forschungszwecke keine demokratische Kontrolle; den entsprechenden Verfahren fehlt systematische **Transparenz**.[35] Bei einer (teilweisen) Bündelung der bisherigen Aufgaben von Ministerien, Aufsichtsbehörden und Ethik-Kommissionen in eigens dafür eingerichteten und untereinander vernetzten UACs ließe sich dieser Missstand durch den Betrieb eines öffentlich einsehbaren Forschungsregisters beheben, an das die UAC wesentliche Informationen zu den von ihnen freigegebenen Forschungsprojekten weitergeben. Dieses Register würde insbesondere den Datenspendern einen Überblick über die Forschung mit ihren Daten, die dafür jeweils Verantwortlichen, ihre Ziele und Fragestellungen sowie die in der Forschung ergriffenen grundrechtsschützenden Maßnahmen erlauben. Nicht zuletzt könnte damit auch der immer wieder erhobenen Forderung nach stärkerer Teilhabe der Patienten und Probanden Rechnung getragen werden.

Durch eine bundesweit einheitliche Regelung in einem **Bund-Länder-Staatsvertrag** könnten die bisherigen, teilweise verstreuten und widersprüchlichen Bundes- und Länderregelungen zur medizinischen Forschung ersatzlos wegfallen. In besagtem Staatsvertrag würden die materiell-rechtlichen und prozeduralen Voraussetzungen für die Zulässigkeit medizinischer Forschungsvorhaben normiert – einschließlich eventueller Einwilligungserfordernisse, der Verfahren der UACs, der Einbindung von Ethik-Kommissionen und Datenschutzaufsicht sowie der Transparenzverpflichtungen gegenüber der Öffentlichkeit.

Die Anregung zur Einrichtung unabhängiger UACs für medizinische Forschungsdaten basiert neben inhaltlichen Erwägungen auch auf der Notwendigkeit, Doppelentwicklungen und Parallelstrukturen in diesem wichtigen und sensiblen Bereich zu vermeiden. Seit Juli 2017 fördert das Bundesministerium für Bildung und Forschung (BMBF) umfänglich die **Medizininformatik-Initiative**, in der zunächst 17 deutsche Universitätskliniken gemeinsam mit externen Partnern so genannte „Datenintegrationszentren“ (DIZ) zum standortübergreifenden Managen und Teilen medizinischer Daten aufbauen.[36] Die geförderten Standorte sind in vier Konsortien organisiert, die im Laufe der kommenden Monate noch weitere, bislang nicht geförderte Universitätskliniken aufnehmen werden. Alle vier Konsortien sehen in ihren Konzepten in der einen oder anderen Weise auch Mechanismen vor, um den Zugang zu den zu teilenden Daten formal auszugestalten. Die Etablierung solcher Verfahren wird sogar eine conditio sine qua non der Funktionsfähigkeit der DIZ sein. Da die überwiegende Mehrheit der deutschen Universitätskliniken absehbar in einem der Konsortien der Medizininformatik-Initiative Aufnahme finden wird, scheint die Einbindung der akademischen medizinischen Forschungslandschaft in angemessene Regelungsmechanismen gesichert. Angesichts dessen wäre es nicht sinnvoll, zusätzliche und von der Medizininformatik-Initiative entkoppelte Verfahren zu etablieren. Vielmehr sollten die Verfahren der Medizininformatik-Initiative so entwickelt und rechtlich gesteuert werden, dass sie sich nach hinreichender praktischer Bewährung auch auf andere forschungsrelevante Medizinbereiche übertragen lassen.

Welche Forschungsprojekte unabhängig vom Datenzugang melde- bzw. genehmigungspflichtig sein sollen bzw. können, bedarf der weiteren fachlichen Erörterung. Maßgebliches Kriterium wird dabei zweifellos die Sensitivität des jeweiligen Projektes sein.

- Auf eine **Meldung und Registrierung kann verzichtet** werden, wenn klassische Eigenforschung erfolgt oder die Forschungsdatenverarbeitung auf einer informierten Einwilligung der Betroffenen basiert.
- **Melde- und registrierungspflichtig** sollten Projekte sein, bei denen eine Interessenabwägung die Betroffeneneinwilligung ersetzen soll, was impliziert, dass die UACs bei solchen Projekten neben Aufklärungs- auch Untersagungsrechte haben müssen.
- Zusätzlich zur bestehenden Meldepflicht sollten Projekte **genehmigungspflichtig** sein, wenn in ihnen hochsensitive Daten verarbeitet werden, wie dies z. B. bei umfangreichen Gensequenzierungen der Fall ist, oder wenn weiterreichende Zweckände-

rungen beabsichtigt sind. Auch zeitlich unbegrenzte Studien[37] bzw. Forschungsdatenbanken sollten unter Genehmigungsvorbehalt gestellt werden.

Für ethisch oder technisch besonders anspruchsvolle Projekte wie z. B. internationale Studien, Forschungsnetzwerke, Krankheitsregister oder Biomaterialdatenbanken[38] könnten vom zuständigen UAC bei Bedarf zusätzliche Anforderungen festgelegt und zur Genehmigungsgrundlage gemacht werden.

7 Schlussbemerkungen

Das vorgeschlagene Regelungsverfahren kann nicht vom Schreibtisch aus geschaffen werden. Vielmehr ist hierfür ein umfangreicher Diskussions- und Abstimmungsprozess unter Einbindung aller Betroffenen erforderlich. Die genaue Ausgestaltung der UACs muss auf den in der Vergangenheit gemachten Erfahrungen basieren und einem strukturierten Prozess folgen, an dessen Ende eine gesetzliche Festlegung stehen sollte. Wie vom Rat für InformationsInfrastrukturen (RfII) gefordert, sollte dieser Entwicklungsprozess Hand in Hand mit dem Aufbau einer netzwerkförmigen Nationalen Forschungsdateninfrastruktur (NFDI) erfolgen.[39]

Der Wissenschaftsstandort Deutschland leidet im internationalen Wettbewerb seit Jahren unter dem Fehlen einheitlicher gesetzlicher Rahmenbedingungen, die ein **zukunftsgerichtetes Forschen an Gesundheitsdaten** unter gleichzeitiger Wahrung der Grundrechte der betroffenen Menschen ermöglichen. Dadurch ergeben sich Nachteile für die wirtschaftliche Entwicklung, den gesellschaftlichen Fortschritt und den Grundrechtsschutz der Menschen. Durch das vorgeschlagene Regelungsverfahren könnte diese Blockade aufgelöst werden. Zugleich würden Erfahrungen gesammelt, die auch in einem größeren einheitlichen Rechtsraum, z. B. in der Europäischen Union, nutzbar gemacht werden könnten.

1 http://www.rfii.de/?wpdmdl=2249.

2 https://gmds.de/fileadmin/user_upload/170511_Memorandum_zum_Datenschutz.pdf.

3 Zu den Datenquellen ausführlicher Weichert DuD 2014, 833.

4 Rienhoff, EHEALTHCom 02_03/16, 26.

5 Schneider, Sekundärnutzung klinischer Daten, 2015, S. 344.

6 Ausführlich zu den für Kliniken geltenden Regelungen Schneider, Sekundärnutzung klinischer Daten, 2015, S. 82 ff., 244 f., 247 f., 310 ff., 323; vgl. auch die unterschiedlichen Anforderungen im Sozialrecht § 75 SGB X, § 287 SGB V, § 98 SGB XI, § 119 SGB XII; zur Regelungsnotwendigkeit auch Stellungnahmen zum Entwurf DSAnpUG-EU der Bundesärztekammer v. 21.03.2017, Deutscher Bundestag, Innenausschuss Ausschussdrucksache 18(4)826, S. 6 f. sowie Deutscher Wissenschaftseinrichtungen, u. a. Deutsche Forschungsgemeinschaft v. 16.02.2017, Ausschussdrucksache 18(4)779 neu S. 3 ff.

7 Netzwerk Datenschutzexpertise, Datenschutzrechtlicher Handlungsbedarf 2016 für die deutsche Politik nach Verabschiedung der EU, Stand 09.05.2016, http://www.netzwerk-datenschutzexpertise.de/sites/default/files/empf_2016_nat_regelungsbedarf.pdf.

8 Dierks, EHEALTHCom 02_03/16, 42.

9 Weichert, „Sensitive Daten“ revisited, DuD 2017, 542.

10 Weichert in Kühling/Buchner, Datenschutz-Grundverordnung (DS-GVO), 2017, Art. 9 Rn. 146-148.

11 Vgl. Wolters, Datenschutz und medizinische Forschungsfreiheit, 1989; Bochnik MedR 1994, 398 ff., 1996, 262 ff. und Weichert MedR 1996, 258 ff.

12 Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V (gmds)/Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD), Positionspapier zur Neugestaltung der datenschutzrechtlichen Regelungen bzgl. der Verarbeitung von personenbezogenen Daten in der Versorgung, Qualitätssicherung und Forschung im Gesundheitswesen, Stand 15.08.2016; Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSB-K), 18./19.03.2015, Nachbesserungen beim eHealth-Gesetz und klare Regelungen zum Einsatz externer Dienstleister bei Berufsgeheimnisträgern erforderlich.

13 Rehborn in Prütting, Medizinrecht, 3. Aufl. 2014, § 15 MBOÄ.

14 BVerfG NJW 1984, 419, 422.

15 BVerfG NJW 1984, 419, 422.

16. RfII, Diskussionspapier, 27.10.2016, S. 10.

17 RfII, Diskussionspapier, 27.10.2016, S. 11.

18 RfII, Diskussionspapier, 27.10.2016, S. 3; RfII, Leistung aus Vielfalt, S. 45 ff.; RfII, Empfehlungen, März 2017, S. 4.

19 World Medical Association (WMA), Declaration of Taipei on Ethical Considerations regarding Health Databases and Biobank, revised by the 67th General Assembly, Taipei, Taiwan, October 2016.

20 CPME endorses the WMA Declaration of Taipei on ethical considerations regarding health databases and biobanks, Press Release 12 April 2017.

21 RfII, Empfehlungen, März 2017, S. 10.

22 Vgl. § 40 Abs. 1 BDSG-alt; § 22 Abs. 1, 2, 5 LDSG SH; Art. 5 Abs. 1 lit. c u. e, 89 Abs. 1 DSGVO.

23 Art. 25, 32 DSGVO; Rost, die Schutzziele des Datenschutzes, in Schmidt/Weichert, Datenschutz, 2012, 353 ff.

24 Weichert, Big Data, Gesundheit und der Datenschutz, DuD 2014, 835.

25 Vgl. z. B. § 28 Abs. 6 Nr. 4 BDSG-alt, § 22 Abs. 4 S. 1 LDSG SH; Art. 7, 9 Abs. 2 lit. a DSGVO.

26 Vgl. § 40 Abs. 3 BDSG-alt; § 22 Abs. 6 LDSG SH.

27 Zum Obigen detaillierter Metschke/Wellbrock, Datenschutz in Wissenschaft und Forschung, 2000; Weichert in Däubler/Klebe/Wedde/Weichert, Bundesdatenschutzgesetz, 2016, § 40.

28 S. o. 3; näher dazu Dochow GesR 2016, 408; Hauser/Haag Datenschutz im Krankenhaus, 4. Aufl. 2012, S. 13; Kircher in Kingreen/Kühling, Gesundheitsdatenschutzrecht, 2015, S. 204, zum Sozialdatenschutz 212 f.; Dix in Simitis, Bundesdatenschutzgesetz, 8. Aufl. 2014, § 1 Rn. 176 ff.; im Ergebnis ebenso Buchner in Buchner, Datenschutz im Gesundheitswesen, Stand 5/2016, A/1 S. 18; aA Uwer in Wolff/Brink, Datenschutzrecht, 2013, Syst. F Rn. 14 f.; Lippert in Ratzel/Lippert MBO-Ä, 5. Aufl. 2010, § 9 Rn. 68, wonach Berufsgeheimnisse dem Datenschutzrecht vorgehen sollen.

29 Als Gehilfen i. S. v. § 203 Abs. 3 S. 2 StGB.

30 Haag/Hauser, Datenschutz im Krankenhaus, S. 22, 254 ff.; Torbohm u. Kingreen/Kühling in Kingreen/Kühling, Gesundheitsdatenschutzrecht, S. 369 f., 446 f.

31 RfII, Empfehlungen, März 2017, S. 19, 23.

32 Z. B. § 22 Abs. 3 Nr. 3, Abs. 4 LDSG.

33 Ähnlich RfII, Empfehlungen, März 2017, S. 13 ff.

34 Technologie- und Methodenplattform für die vernetzte medizinische Forschung e.V. (TMF), http://www.tmf-ev.de/, wahr;

vgl. Pommerening/Drepper/Helbing/Ganslandt, Leitfaden zum Datenschutz in medizinischen Forschungsprojekten, 2014; der Rat für InformationsInfrastrukturen (RfII), Diskussionspapier, 27.10.2016, S. 20 verfolgt ein ähnliches Konzept mit mehreren interdisziplinären Gremien.

35 Weichert DuD 2014, 837.

36 https://www.bmbf.de/de/bessere-therapien-dank-medizininformatik-4473.html

37 Leopoldina/acatech/Union der Akademien der Wissenschaften, Wissenschaftliche und gesellschaftliche Bedeutung von Längsschnittstudien, Mai 2016.

38 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Datentreuhänderschaft in der Biobank-Forschung, 2009.

39 RfII, Leistung aus Vielfalt, 2016, S. 48 f.

Thilo Weichert

Sensorik, automatische Entscheidungen und Persönlichkeitsschutz

Automatisierte Mensch-Technik-Interaktion ist eine neue technische Anwendung, die stark in die Grundrechte der beteiligten Menschen eingreifen kann und daher der Regulierung bedarf. Der Beitrag stellt verfassungsrechtliche Grundlagen hierfür dar und erläutert anhand datenschutzrechtlicher Instrumente wesentliche normative Maßnahmen, mit denen der Persönlichkeitsschutz der betroffenen Menschen gesichert werden kann.

1 Das Phänomen

Die **Digitalisierung** hat inzwischen viele unserer Lebensbereiche erfasst. Beim Mobile Computing führen wir kleine Rechner mit uns, die für uns messen, Wege weisen, Informationen vermitteln und Entscheidungen treffen. Wir tauschen uns in Social Communities aus und hinterlassen dort teilweise sensitive Informationen. Über das Cloud Computing verlagern wir unsere persönliche Datenverarbeitung ins Netz und halten diese weltweit für uns wie für andere verfügbar. Analytics, möglicherweise auf der Grundlage großer Datenmengen – dem Big Data – lässt uns gewaltige Datenmengen durchdringen, um diese auf spezifische Fragestellungen hin zu untersuchen und auf dieser Grundlage – evtl. in Echtzeit – Entscheidungen zu treffen oder vom Rechner treffen zu lassen.

Die **technische Entwicklung** geht ungebrochen weiter. Gab es noch bis vor kurzem eine logische Trennung zwischen digitaler und analoger Welt, so wird diese nun aufgehoben. Einen gewaltigen Beitrag hierfür liefert die Sensorik, die analoge Sachverhalte in digitale Informationen umwandelt. Dies beginnt mit der Messung äußerer Sachverhalte wie Temperatur und Umweltsituation, geht über individuelle Sachverhalte wie die sportliche Betätigung oder den Gesundheitszustand und über die derzeit in Mode geratenden Sprachassistenten bis hin zu genetischen Befunden über körperliche oder seelische Dispositionen. Mit Hilfe von Virtual oder Augmented Reality werden unsere Wahrnehmungsmöglichkeiten erweitert, wird unsere Vorstellung von der analogen Welt qualifiziert. Mit Hilfe von Mensch-Maschine-Schnittstellen werden nicht nur unsere Wahrnehmungs- sondern auch unsere Handlungsfähigkeiten erweitert. Behinderungen werden aufgehoben. Der Computer und daran angeschlossene Maschinen ermöglichen Aktivitäten, welche die Natur nicht für uns vorgesehen hat. Cyborgs, die Kombination von Mensch und Maschine in einer Einheit, werden möglich. Roboter, die von Menschen bisher ausgeübte Tätigkeiten eigenständig durchführen, ziehen in unseren Alltag ein und rücken uns auf den Leib.

Der Schlüssel für diese Entwicklungen ist der informationstechnische Fortschritt. Der Umfang von Datenbeständen ist kaum noch eine Beschränkung bei der Erhebung, Speicherung und Auswertung in Echtzeit. Selbst komplexe Sachverhalte und unterschiedliche Formate lassen sich automatisiert zusammenführen und umgehend analysieren. Die Informationstechnik ist geprägt von „volume“, „variety“ und „velocity“. Hinzu kommt ein Phänomen, das mit dem Begriff **„künstliche Intelligenz“** beschrieben wird. Intelligenz, eine bisher ausschließlich dem Menschen und einigen höher entwickelten Tierarten zugeschriebene Fähigkeit, wird auf Computer zu übertragen versucht. Die dahinter steckende Intention ist es, die Welt besser zu machen, Mehrwert („value“) für Kapitalanleger und möglicherweise auch für die Menschen allgemein zu schaffen. Mit der Digitalisierung werden Heilsversprechungen verknüpft, im medizinischen Bereich auch Heilungsversprechen. Es kommt zu personalisierten Anwendungen, also den einzelnen Menschen direkt treffenden spezifischen Effekten.

Die Interaktion zwischen Mensch und Maschine erfolgt schon heute bei vielen Gelegenheiten in der **Welt der Wirtschaft**, insbesondere über Werbung und die Manipulation von Bedürfnissen. Im Netz tätige Roboter, kurz Bots genannt, beeinflussen unser Konsumverhalten und unsere Art der Informationsbeschaffung und der Kommunikation. Sie werden meinungs- und verhaltenslenkend,

nicht nur beim Konsum, sondern selbst in der Politik. Eine spezifische Form des Konsums ist die Unterhaltung und das Spiel, wofür die Menschen dank der automationsbedingten Entlastung von körperlicher und geistiger Anstrengung zunehmend Zeit und steigenden Bedarf haben. Die Verknüpfung des analogen Menschen mit digitalen Prozessen dient auch existenziellen individuellen und gesellschaftlichen Zielen, etwa in der computerisierten Medizin mit digitaler Diagnose, Behandlung und Nachsorge. Handicaps werden mit digitaler Hilfe behoben oder zumindest gemildert. Im Bereich der Pflege ist Dauerüberwachung und zeitnahe Intervention möglich.

Völlig **neue Perspektiven** eröffnen sich auch z. B. im Verkehr, wo nach dem automatisierten das autonome Fahren zum Ziel erklärt worden ist. Sicherheitsbehörden können mit Computerhilfe Risiken präventiv erfassen und beheben sowie Regelverstöße im Nachhinein beweissicher feststellen und sanktionieren. Eine technische Revolution erfolgt in der Arbeitswelt. Der Mensch als solcher verliert für die Produktion und selbst im Bereich der Dienstleistungen an Bedeutung und wird oft nur noch als intelligente Verlängerung der Maschine benötigt.

2 Risiken

Neben den erwünschten Effekten ergeben sich bei dieser Digitalisierung auch unerwünschte Auswirkungen. Der Einsatz der Informationstechnik verändert die Kommunikations- und Machtbeziehungen zwischen den Menschen und in der Gesellschaft. Diese Auswirkungen lassen sich wie folgt knapp zusammenfassen:

- Die digitale Erhebung von Daten macht diese allgemein verfügbar und gefährdet damit deren **Vertraulichkeit**.
- Durch die vorgegebene Analyse der Daten und deren Verwendung für Entscheidungen wird die **Freiheit** der Menschen hierbei und in deren Wahloptionen beschränkt.
- Diese Beschränkungen können bis zum Ausschluss führen, also zur **Diskriminierung** auf Grund bestimmter Eigenschaften und Merkmale.
- Nicht weniger problematisch ist die gezielte Beeinflussung, d. h. die **Manipulation** von Menschen durch die Beeinflussung der Gefühle oder durch die Vorgabe von nicht änderbaren Rahmenbedingungen.
- **Seelische und körperliche Schäden** können dadurch entstehen, dass über die Manipulation und Diskriminierung das Potenzial der einzelnen Menschen eingeschränkt wird.
- Hieraus können **finanzielle oder materielle Schäden** resultieren.
- Eine spezifische Form der materiell-finanziellen Schädigung besteht in der **kommerziellen Ausbeutung**, also der profitorientierten Manipulation des Konsums.

Nicht nur für den Einzelnen, auch für die Informationstechnik einsetzenden **Stellen bzw. Unternehmen** ergeben sich Risiken der Ausspähung z. B. von Betriebs- und Geschäftsgeheimnissen, der Sabotage und der Rufschädigung, was zum Totalausfall von Funktionalitäten und zu massiven wirtschaftlichen Beeinträchtigungen führen kann.

3 Verfassungsrechtliche Grundlagen

Das **Grundgesetz** (GG) stammt in seinen Kerninhalten aus dem Jahr 1949, also bevor die Digitalisierung des Lebens begann, und gibt keine Antworten auf damit entstehenden neuen Herausforderungen. Wohl aber benennt das GG die Werte, die bei gesellschaftlichen Entwicklungen und bei technischem Fortschritt beachtet werden müssen. An vorderster Stelle steht der Schutz und die Wahrung der menschlichen Würde (Art. 1 Abs. 1 GG) sowie der allgemeinen Handlungsfreiheit (Art. 2 Abs. 1 GG), woraus das deutsche Bundesverfassungsgericht schon im Jahr 1983 ein Grundrecht auf informationelle Selbstbestimmung abgeleitet hat. Sämtliche individuellen und politischen Freiheitsrechte können immateriell oder materiell tangiert sein – von der Glaubens- und Gewissensfreiheit bis zum Schutz des Eigentums. Als spezifisches Grundrecht an der Schnittstelle zwischen Mensch und Maschine ist das Recht auf körperliche Unversehrtheit zu nennen (Art. 2 Abs. 2 GG). Die Unversehrtheit der körperlichen Sphäre ist nicht die einzige zu schützende individuelle Sphäre: Schutzbedarf besteht auch in Bezug auf die Familiensphäre (Art. 5 GG), die räumliche Sphäre der Wohnung (Art. 13 GG); neu hinzugekommen ist mit dem Urteil des BVerfG zur Online-Durchsuchung (U. v. 27.02.2008, 1 BvR 370/07, 1 BvR 595/07) die individuelle „digitale Sphäre“, die durch das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ ihre rechtliche Fundierung und Präzisierung gefunden hat.

Die individuellen Grundrechte haben auch **gesellschaftliche Funktionen**. Diese finden ihren Ausdruck im Gleichheitsgrundsatz und in den Diskriminierungsverboten, im Sozialstaats- und Demokratiegebot (Art. 20 GG) sowie in der Rechtsschutzgarantie (Art. 19 Abs. 4 GG). Die Grundrechte verpflichten nicht nur staatliche Einrichtungen direkt bei deren Eingriffsverwaltung, sondern auch dazu, die Rahmenbedingungen für deren Verwirklichung zu schaffen. Dem Staat obliegt eine Schutz- und Fürsorgepflicht, die durch Institutionen und Regeln umgesetzt werden muss und über die auch private Stellen und Personen veranlasst werden, die Grundwerte der Verfassung zu beachten (sog. Drittwirkung von Grundrechten).

Der normative Rahmen des Grundgesetzes hat mit der **europäischen Grundrechte-Charta** (GRCh) Aktualisierung, Modernisierung und Anpassung an die technische Realität erfahren. Neben der Bestätigung der klassischen Grund- und Freiheitsrechte (Privatheit, Familie, Wohnung, Kommunikation, Art. 7, Gedanken-, Gewissens- und Religionsfreiheit, Art. 10, Meinungs-, Informations-, Vereinigungs- und Versammlungsfreiheit, Art. 11, 12) wurde das Recht auf informationelle Selbstbestimmung als Grundrecht auf Datenschutz explizit kodifiziert (Art. 8 GRCh). Der Zugang zu Dokumenten bzw. generell zu Informationen findet eine ausdrückliche Grundlage (Art. 42 GRCh) ebenso wie der Verbraucherschutz (Art. 38 GRCh).

4 Herausforderungen

Dieser normative Rahmen muss bei der Gestaltung der Mensch-Maschine-Kommunikation, also der Schnittstelle zwischen analoger Realität des Menschen und seiner Umwelt und dessen digitaler Begleitung, berücksichtigt werden. Mit

der Digitalisierung werden neue Geschäftsmodelle geschaffen und eröffnen sich Profitmöglichkeiten. Doch muss bzw. sollte sie zugleich auch einen Beitrag zur Bewältigung der in der modernen Welt bestehenden, teilweise globalen Herausforderungen leisten. Die Erwartung besteht, dass über die Digitalisierung neue Antworten gegeben werden können auf die Umweltverschmutzung und -zerstörung, die Veränderung des Klimas, zur Sicherung der Ernährung der Bevölkerung oder zur Wahrung des Friedens und der Solidarität in der Gesellschaft. Manche insofern gemachten Versprechen erweisen sich als Irrtum. Es ist aber offensichtlich, dass die Digitalisierung Beiträge zur Lösung dieser Probleme leisten kann. Angesichts der Komplexität der Probleme und des Umfangs der für die Lösung relevanten Datengrundlage ist die Nutzung digitaler Hilfsmittel hierfür sogar unabdingbar.

Was für die Gesellschaft allgemein gilt, gilt auch für den einzelnen Menschen. Mit der Mensch-Maschine-Kommunikation wird insbesondere ein **individueller Automationsansatz** für die einzelnen Nutzenden bzw. Anwender verfolgt mit wichtigen positiven Effekten:

- Für den Konsumenten wie den Arbeitnehmer steht die **Komfortverbesserung** im Vordergrund: Durch die Automation der Mensch-Maschine-Schnittstelle kann die Bedienung erleichtert und der Automationseinsatz in Bezug auf „Intelligenz“, Geschwindigkeit und Funktionalität optimiert werden.
- Dies hat sowohl für die Anbieter der Dienste wie auch für die Unternehmen, bei denen solche Dienste zum Einsatz kommen, eine **Produktivitätssteigerung** und eine Erhöhung der Wettbewerbsfähigkeit zur Folge.
- Ein weiterer Effekt kann darin liegen, die **Anwendungssicherheit** des IKT-unterstützten Verfahrens zu erhöhen. Sind die nötigen Maßnahmen zur Datensicherheit ergriffen und besteht eine funktionale Programmierung, so sind automatisierte Systeme zumeist weniger fehleranfällig, vorausgesetzt die jeweilige Sicherheitslage ist überhaupt automatisierungsfähig.

Während es in den Frühzeiten der Digitalisierung bei der Schnittstelle zwischen Mensch und Maschine (Computer) einen Medienbruch gab, wird dieser mit neuen Techniken ganz oder teilweise aufgehoben. Das am weitesten verbreitete Beispiel sind Sprachassistenten, wie sie inzwischen für den Hausgebrauch von allen großen US-Plattformen angeboten werden von Amazons Alexa bzw. Echo über Google Home, Microsofts Cortana bis zu Apples Siri bzw. PodHome. Weitere Beispiele **gewillkürter Schnittstellenautomation** sind der Einsatz implantierter Chips, die Bedienung von Rechnern mit Hilfe von bestimmten Körperbewegungen (z. B. Lidschlag) oder – noch in einem frühen Entwicklungsstadium – die Computersteuerung mit Gedanken. Gegenüber der klassischen Tastatureingabe verflüchtigt sich bei derartigen Techniken mit dem Komfort- und Funktionalitätsgewinn die Explizitheit der Eingabe, da mit Sensoren gekoppelte Algorithmen den menschlichen Willen interpretieren, statt diesen – wie bei manueller Eingabe – direkt umzusetzen.

Eine weitere Stufe wird mit Sensoren erreicht, die nicht **mehr gewillkürte Handlungen** eines Menschen digitalisieren, sondern mechanische, chemische oder biotechnische Zustände. Ein Beispiel hierfür ist der Aufmerksamkeitssensor im Auto, der den Lidschlag des Fahrers misst und interpretiert. Ein medizinisches Beispiel ist die automatisierte Insulinabgabe bei Diabetes-Patienten. Weitere Beispiele sind medizinische Diagnosen auf der Grundlage von Stimmanalysen oder die Emotionserfassung durch Gesichtsanalyse.

Bei der Automatisierung der Mensch-Maschine-Kommunikation sind die sozialen und individuellen Rahmenbedingungen zu beachten, die bei jeder Form der Digitalisierung auftreten und die durch rechtliche, organisatorische sowie technische Maßnahmen unter Kontrolle gebracht werden können. Die **Besonderheiten** dieser Kommunikationsform machen zusätzliche spezifische Vorkehrungen zur Wahrung der digitalen Souveränität nötig:

- Die Mensch-Maschine-Kommunikation zielt darauf ab, menschliche Gedanken zu erfassen und hieraus Entscheidungen abzuleiten. Erfasst werden damit nicht nur Äußerlichkeiten einer Person, sondern auch deren Wertungen und Entscheidungen, denen eine höhere persönlichkeitsrechtliche Sensitivität zukommt.
- Dies gilt erst recht, wenn nicht nur bewusste, sondern auch un- bzw. unterbewusste innere Vorgänge der Personen erfasst werden. Gefühle waren bisher personale Sachverhalte, die einer Erfassung und Auswertung nur sehr begrenzt zugänglich waren. Dies hat sich mit der Automation der Mensch-Maschine-Beziehung geändert.
- Diese qualitative Änderung ist verbunden mit einer spezifischen Fehleranfälligkeit, die aus der Interpretationsbedürftigkeit der sensorisch erfassten menschlichen Regungen resultiert. Die Interpretation, z. B. mit Instrumenten künstlicher Intelligenz, basiert in jedem Fall ausschließlich auf den programmtechnischen Vorgaben sowie dem eingegebenen Datenbestand.
- Trotz dieser doppelten Fehlerquellen hat die automatisierte Interpretation menschlichen Verhaltens den Nimbus der Wissenschaftlichkeit und damit der Objektivität. Dies begünstigt die Bereitschaft der Nutzenden, die Verantwortung für getroffene Feststellungen und Entscheidungen dem Rechner zu überlassen.
- Aus der scheinbar wissenschaftlichen und der faktisch-technischen Objektivität der Digitalisierung menschlicher Regungen ergibt sich das Problem, dass die digitale Erfassung vom freien Willen des Betroffenen losgelöst wird. Zwar kann es die Zielsetzung der automatisierten Schnittstelle sein, diesen freien Willen bestmöglich zu erfassen. Dies ändert aber nichts an dem Umstand, dass dies nur über formalisierte und standardisierte Automation erfolgen kann: Die Erfassung der menschlichen Regungen wird zwangsläufig, quasi „schicksalhaft“.
- Die Vorgänge der Erfassung bis hin zur Interpretation erfolgen dabei in einer für den Betroffenen oft intransparenten, und zumeist auch nicht mehr nachvollziehbaren Weise. An die Stelle informationeller Selbstbestimmung droht die Fremdbestimmung durch den digitalen Code zu treten.

5 Datenschutz-Grundprinzipien

Bevor aus diesen Besonderheiten normative Konsequenzen gezogen werden,

sollen zunächst überblicksmäßig die allgemeinen rechtlichen und technischen Grundlagen des Datenschutzes dargestellt werden, auf denen spezifische Maßnahmen zur Mensch-Maschine-Kommunikation aufsetzen. Dabei handelt es sich um folgende Grundsätze:

- Der Grundsatz der **Rechtmäßigkeit** (Art. 5 Abs. 1 lit. a, 6 DSGVO, § 28 BDSG-alt) besagt, dass jede Form personenbezogener Datenverarbeitung einer normativen Legitimation bedarf, also entweder einer Einwilligung oder einer gesetzlichen Grundlage.
- Das Erfordernis der **Einwilligung und der Wahlfreiheit** (Art. 7 DSGVO, § 4a BDSG-alt) realisiert die informationelle Selbstbestimmung in den Fällen, in denen die Betroffenen einen konkreten Bezug zur sie betreffenden Verarbeitung herstellen (können/wollen).
- Der Grundsatz der **Zweckbindung** (Art. 5 Abs.1 lit. b, 6 Abs. 4 DSGVO) soll gewährleisten, dass Daten nur für die Zwecke verwendet werden, für die sie erhoben wurden und dass bei der Weiterverarbeitung keine mit diesen Zwecken unvereinbare Ziele verfolgt werden.
- Die **Richtigkeit** (Art. 5 Abs. 1 lit. d, 16 DSGVO, § 35 BDSG-alt) hat die Wahrheitsgemäßheit der digitalen Abbildung zum Ziel.
- Mit den Prinzipien der **Erforderlichkeit** bzw. der Datensparsamkeit (Art. 5 Abs. 1 lit. c, e DSGVO, § 3a BDSG-alt) erfolgt eine persönlichkeitsrechtliche Risikominimierung durch die Vermeidung unnötiger, evtl. schädlicher Daten.
- **Betroffenenrechte** (Art. 5 Abs. 1 lit. a, 12 ff. DSGVO, §§ 33, 34 BDSG-alt: v. a. Auskunft, Berichtigung, Löschung) sind grundlegende Voraussetzungen digitaler Souveränität, insbesondere für die Betroffenen, aber auch für die Verantwortlichen sowie sonstige Beteiligte.
- Mit dem Erfordernis der **Datensicherheit** (Art. 5 Abs. 1 lit, f, 25, 32 ff. DSGVO, § 9 BDSG-alt) werden die technischen Grundlagen zur Umsetzung des Datenschutzes gesetzt.
- Es muss in jedem Fall gewährleistet sein, dass einer Person, einer Stelle oder mehreren Stellen die **Verantwortlichkeit** für einen digitalen Vorgang zukommt und rechtlich wie auch tatsächlich überwiesen wird (Art. 5 Abs. 2, 24 ff. DSGVO, § 3 Abs. 7 BDSG-alt).
- Von staatlicher Seite soll durch die **Datenschutzkontrolle** (Art. 37 ff, 51 ff. DSGVO, § 38 BDSG-alt) die Übernahme der Verantwortung für die Informationsverarbeitung gesichert werden.

Um diese normativen Vorgaben umzusetzen, müssen die Technik und das die Technik einsetzende Verfahren so gestaltet werden, dass folgende **Schutzziele** zueinander in einem optimalen Verhältnis verwirklicht werden können:

- Die Wahrung der **Vertraulichkeit** der Daten kann z. B. über deren Verschlüsselung, durch qualifizierte Zugriffskonzepte oder durch räumliche oder logische Trennung erreicht werden.
- Die **Datenintegrität** bzw. Authentizität lässt sich durch zertifizierte Verfahren der Verarbeitung, durch Maßnahmen der Qualitätssicherung oder durch die digitale Signierung von Datensätzen gewährleisten.
- Mit der **Datenverfügbarkeit** wird sichergestellt, dass die Funktion der Verarbeitung durch Datenverlust nicht beeinträchtigt wird. Dem kann durch Replizierung der Daten (Backups) sowie durch Redundanz der Verarbeitungssysteme (bis zur Sicherung der Stromversorgung) genügt werden.
- **Intervenierbarkeit** zielt auf die (persönlichkeitsrechtsbedingte) Veränderbarkeit des Datenbestandes oder einzelner Daten, also z. B. die spezifische Sperr- und Löschbarkeit.
- Mit der **Transparenz** durch Dokumentation und Protokollierung wird die Datenverarbeitung revisionsfähig gemacht, um die digitalen Vorgänge sowie die Verantwortlichkeiten hierfür feststellen und prüfen zu können.
- Technische und organisatorische Maßnahmen zur **Nichtverkettbarkeit**, etwa über eine File- oder Mandantentrennung, über Rollenkonzepte, Abschottungen und Treuhändermodelle haben die Absicherung des Zweckbindungsgrundsatzes zum Ziel.

Bei Mensch-Maschine-Systemen darf – wie bei anderen komplexen Technikeinsätzen – nicht alles gemacht werden, was möglich ist. Dies gilt nicht nur aus ethischen Erwägungen, sondern auch im rechtlichen Sinn. Eine absolute Grenze, die nicht überschritten werden darf, ist der **Kernbereich privater Lebensgestaltung**. Dieser darf weder von privaten Stellen noch vom Staat verletzt werden. Die Gefährdung dieses Kernbereichs kann sogar dazu verpflichten, dass der Betroffene daran gehindert wird bzw. werden muss, über sich zu disponieren. Dieses absolute rechtliche Tabu speist sich rechtsdogmatisch aus dem Würdeschutz (Art. 1 Abs. 1 GG, Art. 1 GRCh) sowie aus den Freiheitsrechten, deren Wesensgehalt nicht beeinträchtigt werden darf. Gemäß der ständigen Rechtsprechung des Bundesverfassungsgerichts seit dem „Elfes-Urteil“ (U. v. 16.01.1957, 1 BvR 253/56) wird damit ein „letzter unantastbarer Bereich menschlicher Freiheit“ beschrieben.

Worin dieser Kernbereich besteht, kann nicht zeitlos und unabhängig von den **bestehenden Umwelt- und Lebensbedingungen** definiert werden. Angesichts der technischen Entwicklung geht es darum, die Objektivierung des Menschen wie auch das Eindringen in den intimsten höchstpersönlichen Bereich der Menschen zu verhindern oder zumindest einzuschränken. Erfasst wird vom Kernbereich teilweise auch soziales Handeln, etwa in besonders geschützten Bereichen (Familie, Wohnung, Sexualität). Hierzu gehört aber insbesondere der innere Bereich eines Menschen mit seinen Gefühlen und Gedanken. Gerade diese bisher von der Technik unangetastete Sphäre wird mit neuen Mitteln der Mensch-Maschine-Kommunikation zugänglich gemacht. Der Kernbereich privater Lebensgestaltung verbietet nicht pauschal den Einsatz solcher Mittel. Wohl aber muss durch materielle Verbote wie durch prozedurale wie technisch-organisatorische Maßnahmen gesichert werden, dass es bei diesem Mitteleinsatz nicht zum Tabubruch kommt.

6 Technikregulierung

An zwei **Beispielen** soll dargelegt werden, wie dieser Tabubruch normativ verhindert werden soll und kann. Hieraus können dann Schlussfolgerungen für die Mensch-Maschine-Interaktion gezogen werden:

Das erste Beispiel ist das **Gendiagnostikgesetz** (GenDG), mit dem die

Analyse von Gendaten für Zwecke der Medizin und der Abstammungsfeststellung im Arbeitsleben und im Bereich des Versicherungswesens rechtsstaatlich eingehegt wird. Gendaten haben zu neuronalen Daten sowie mit Gedanken und Gefühlen Ähnlichkeiten: Sie sind höchstpersönlich, nicht bzw. nur schwer veränderbar und insofern gegenwärtig und zugleich für die Betroffenen schicksalhaft. Sie haben eine Auswirkung auf die körperliche wie seelische Disposition des Menschen. Ihre Feststellung ist nur sehr beschränkt äußerlich möglich und setzt den Einsatz komplexer wissenschaftlicher, für die Betroffenen zumeist weder nachvollzieh-, geschweige denn verstehbarer Verfahren voraus.

Die **Regulierung** der Gendiagnostik beinhaltet sowohl materiell-rechtliche wie auch technisch-organisatorische und prozedurale Vorkehrungen. Verboten sind spezifische Diskriminierungen. Erlaubt ist nur das Verfolgen abschließend genannter enger Zwecke. Die Qualität des Verfahrens soll durch qualifizierte Anforderungen an die eingesetzten Methoden, die verwendeten Mittel und die handelnden Personen (z. B. Arztvorbehalt) gesichert werden. Der gesamte Lebenszyklus der Daten von deren Erfassung über die Speicherung, Analyse, Nutzung und evtl. Weitergabe bis hin zur Vernichtung ist reguliert. Um ein Maximum an Selbstbestimmung zu gewährleisten, muss ein Höchstmaß an Transparenz für die Betroffenen sowie an Bestimmungsmöglichkeit hergestellt werden durch Aufklärung, Beratung und Zustimmungs- bzw. Widerspruchsmöglichkeiten bis hin zum Recht auf Nichtwissen.

Als zweites Beispiel soll hier die Regulierung von **automatisierten Einzelentscheidungen** aufgeführt werden. Diese sind bisher in Art. 15 EG-Datenschutzrichtlinie sowie in den §§ 6a, 28b BDSG-alt geregelt. Künftig werden Art. 22 Datenschutz-Grundverordnung sowie § 37 BDSG-neu anwendbar sein. Diese Regelungen gelten teilweise direkt auch im Bereich der Mensch-Maschine-Kommunikation, z. B. wenn sensorisch erfasste Daten an einen medizinisch-informationstechnischen Dienstleister transferiert werden, die dann die Grundlage von automatisierten Arzneimittelverordnungen abgeben. Bei solchen automatisierten Entscheidungen ergeben sich rechtliche oder sonstige, evtl. psychologisch vermittelte, Wirkungen, die einen erhöhten Schutzbedarf begründen. Diese setzen regelmäßig eine direkte Einbindung des Betroffenen bei der Einrichtung des Verfahrens (per Einwilligung oder Vertrag) voraus. Sollten hieraus für den Betroffenen gravierende negative Effekte drohen, so muss gewährleistet werden, dass der Betroffene intervenieren und seinen Standpunkt darlegen kann. Dies gilt insbesondere, wenn sensitive Daten einbezogen sind. Das zum Einsatz gebrachte Verfahren muss wissenschaftlichen Anforderungen bei der mathematisch-statistischen Berechnung wie auch hinsichtlich der Wirksysteme genügen. Weitere Voraussetzung ist, dass die Datengrundlagen rechtmäßig generiert wurden und nicht zu Diskriminierungen führen. Das Verfahren ist zu dokumentieren; für die Betroffenen ist die größtmögliche Transparenz herzustellen. Da es sich bei dem vorliegenden Regelungsbereich um ein äußerst dynamisches Feld handelt, müssen weitere anwendungsspezifische Anforderungen in Konkretisierung der genannten allgemeinen Erfordernisse erarbeitet werden.

7 Schlussfolgerungen

Für die Mensch-Maschine-Interaktion lassen sich aus dem oben Dargestellten folgende allgemeine **Anforderungen** übertragen:

- Die mit der Interaktion verfolgten **Zwecke** sind präzise festzulegen.
- Risikobezogen sind die Bereiche zu definieren, mit denen in den **unantastbaren persönlichkeitsrechtlichen Kernbereich** eingedrungen werden kann. Ein Eindringen in diesen Bereich ist durch Verbote, Verfahren und technische Maßnahmen auszuschließen.
- Die **Transparenz** des eingesetzten Verfahrens muss für alle Beteiligten sichergestellt werden. Diese sind neben dem Betroffenen u. a. die verantwortlichen Stellen selbst und die (staatliche) Aufsicht. Neben dieser Transparenz hinsichtlich des konkreten Einsatzes bedarf es einer strukturellen Verfahrenstransparenz, an der die Öffentlichkeit, zumindest aber die Fachöffentlichkeit und die Forschung zu beteiligen ist.
- Die Verfahren sind so zu gestalten, dass es für die Betroffenen ein Höchstmaß an **Interventions- und Wahlmöglichkeit** gibt. Dies bedingt in der Regel eine Skalierbarkeit beim Einsatz und dass die Interaktion durch den Betroffenen jederzeit unterbrochen bzw. eingestellt werden kann.
- Das Verfahren ist so zu gestalten, dass **keine Diskriminierungen** erfolgen.
- Die **Qualität** des Verfahrens ist durch verpflichtende Zertifizierungen und im Betrieb durch regelmäßige Evaluationen/Monitorings/Audits zu überprüfen und sicherzustellen.

Aus dem Vorgesagten zeigt sich, dass digitalisierte Mensch-Maschine-Interaktionen **Regulierungsbedarf** auslösen. Bisher nur in Ansätzen diskutiert ist die Frage, wer insofern in der Pflicht ist. Verfassungsrechtlicher Standard ist, dass alles Wesentliche für die Grundrechtssicherung in einem parlamentarisch beschlossenen Gesetz geregelt sein muss. Es stellt sich aber darüber hinausgehend die Frage, ob sich nicht auch für den Verfassungsgeber Novellierungsbedarf ergibt. Ein solches Anliegen verfolgt der Entwurf einer „Charta der Digitalen Grundrechte der Europäischen Union“ vom November 2016.

Auf der praktischen Seite sind Funktionalität, Nachvollziehbarkeit für die Beteiligten und intuitive Bedienbarkeit zu fordern. Da dies keine Selbstverständlichkeiten sind, ist auch insofern eine rechtliche Fixierung geboten. Dieser Rahmen kann nicht abstrakt entstehen, sondern bedarf einer Entwicklung in einem experimentellen Prozess, an dessen (vorläufigem) Ende für spezifische Szenarios **Standards** festgelegt werden können, welche als Grundlage für verbindliche Festlegungen dienen. Bei der Kodifizierung dieser Standards sollte ein umfassender Ansatz verfolgt werden, bei dem materielle, technische und organisatorisch-prozedurale Festlegungen erfolgen.

Mensch-Maschine-Interaktion ist ein technischer Bereich, der eine weitere rechtliche und praktisch-wissenschaftliche Aufarbeitung nötig macht. Dabei sind weder Laissez-faire noch Maschinensturm angesagt. Im Vordergrund müssen der Nutzen und die Abwehr von Gefahren **für die Menschen** stehen, nicht die Aussicht auf ein gewinnbringendes Geschäftsmodell.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Generalbundesanwalt stellt Vorermittlungen über Snowden-Enthüllungen ein

Mehr als vier Jahre nach dem Beginn der Veröffentlichungen von Edward Snowden zu den NSA-Lauschangriffen sah der Generalbundesanwalt „keine belastbaren Hinweise für eine gegen die Bundesrepublik Deutschland gerichtete geheimdienstliche Agententätigkeit oder andere Straftaten", d. h. auf eine massenhafte und systematische Internetüberwachung und stellte die Untersuchungen u. a. wegen einer Verletzung des Spionage-Paragrafen 99 Strafgesetzbuch (StGB) ein.

Die NSA, der britische GCHQ und andere westliche Geheimdienste greifen in großem Umfang internationale Kommunikation ab, spionieren Unternehmen sowie staatliche Stellen aus und verpflichten Dienstleister im Geheimen zur Kooperation. Einzelheiten dazu hatte Edward Snowden enthüllt. Der Generalbundesanwalt gesteht zwar ein, dass US-amerikanische sowie britische Geheimdienste strategische Fernmeldeaufklärung betreiben und dafür Telekommunikations- und Internetdaten filtern. Aber es gebe „keine belastbaren Anhaltspunkte" dafür, dass „das deutsche Telekommunikations- und Internetaufkommen rechtswidrig systematisch und massenhaft" überwacht werde. Das gelte auch für jene Kommunikation, die über in Deutschland verlaufende Glasfaserkabel abgewickelt werde.

Bei dieser Einschätzung stützt sich der Generalbundesanwalt nach der mehrjährigen Prüfung auf das für die Spionageabwehr zuständige Bundesamt für Verfassungsschutz (BfV), das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Betreiber des De-Cix. Die Snowden-Dokumente, die den NSA-Skandal ausgelöst hatten, hätten keine konkreten Hinweise „auf tatsächlich fassbare Spionagehandlungen der NSA in oder gegen Deutschland ergeben". Sie enthielten lediglich Aussagen zu den Fähigkeiten des US-Nachrichtendienstes, die schon vorher als technisch machbar bekannt gewesen wären. Es gebe keine Belege, dass sie „zielgerichtet gegen Deutschland" eingesetzt würden. Die Dokumente würden auch nicht Aufschluss geben über konkrete, tatsächlich durchgeführte Abhörmaßnahmen, weswegen es keinen Raum für Ermittlungen gebe.

Damit scheint der NSA-Skandal zumindest offiziell auch in Deutschland beendet, wo er im weltweiten Vergleich für besonders viel Aufsehen gesorgt hatte. Nicht zuletzt kam ein Untersuchungsausschuss zustande, der vor der Bundestagswahl im Herbst 2017 seine Arbeit abgeschlossen hat. Dort gab es keine Einigkeit über die Ergebnisse. Wohl aber war in dessen Rahmen mehr über die Kooperation deutscher Geheimdienste mit ausländischen Partnern bekannt geworden. Vor allem auch an der von der NSA veranlassten Überwachung deutscher und europäischer Zielpersonen hatte es viel Kritik gegeben. Dem Generalbundesanwalt reichte das aber offenbar nicht aus. Dass es keine offiziellen strafrechtlichen Ermittlungen geben würde, war bereits kurz nach Einleitung der Vorermittlung absehbar gewesen. Dass die deutschen Stellen die Zusammenarbeit mit den eigenen Diensten und die hier stattfindenden Abhöraktivitäten eher als Dienst im deutschen Interesse sehen denn als Schaden, war dann nicht überraschend. Diese hatten oft erklärt, dass Deutschland in der Terrorabwehr von US-Hilfe abhängig wäre, die ohne Gegenleistung nicht zu haben sei. Es liege im deutschen Interesse, sich am „Geben und Nehmen" mit Partnern „vor allem jenseits des Atlantiks" zu beteiligen, hatte z. B. Hans-Georg Maaßen, Präsident des BfV, am Tag der Bekanntgabe der Einstellungen der Untersuchungen am 05.10.2017 im Bundestag erklärt.

Der Vizechef der Bundestagsfraktion von Bündnis 90/Die Grünen Konstantin von Notz kritisierte: „Jahrelang haben wir im NSA-Untersuchungsausschuss versucht, das massenhafte Abgreifen von Kommunikationsdaten durch die amerikanischen und britischen Geheimdienste aufzuklären." Die Entscheidung der Karlsruher Ermittler nannte er einen „Schlag ins Gesicht für die Bürgerrechte". Die Ermittlungen wegen des mutmaßlich abgehörten Handys der Kanzlerin waren bereits Juni 2015 beendet worden. Auch die beim BND eingespeisten US-Selektoren beschäftigen die Ermittler in Karlsruhe nicht mehr (Holland, NSA-Skandal: Keine Hinweise auf NSA-Spionage – Generalbundesanwalt beendet Untersuchung, www.heise.de 05.10.2017; Steinke, Ermittlungen in der NSA-Affäre eingestellt, SZ 06.10.2017, 1).

Bund

Viele BKA-Datenspeicherungen rechtswidrig

Die Aufklärung des Skandals um den Entzug von Akkreditierungen für JournalistInnen beim G20-Gipfel brachte ans Licht, dass viele Datenspeicherungen im Bundeskriminalamt (BKA) fehlerhaft und rechtswidrig sind bzw. waren.

Björn Kietzmann ist einer der „etlichen Straftäter", mit denen die Bundesregierung den Entzug von 32 Akkreditierungen beim G20-Gipfel in Hamburg begründet hatte. Sein erweitertes polizeiliches Führungszeugnis von 2015 ist blütenweiß. Der Datenauszug, den das BKA dem 37-jährigen Fotografen per Post zusendete, enthält

dagegen gleich 18 Einträge. Ins Auge sticht der Vorwurf „Herbeiführen einer Sprengstoffexplosion“ in der Kategorie „politische motivierte Kriminalität“ – eine der vielen nachweislich falschen Eintragungen: Kietzmann hatte im Juli 2011 eine Demonstration fotografiert, als in seiner Nähe ein Feuerwerkskörper explodierte. Die Polizei hielt ihn für den Täter, nahm ihn fest und ließ ihn erkennungsdienstlich behandeln. Vier Kollegen, mit denen Kietzmann zum Zeitpunkt des Vorfalls zusammenstand, bestätigten gegenüber der Staatsanwaltschaft dessen Unschuld. Die Staatsanwaltschaft reduzierte die Ermittlungen daraufhin vom Vorwurf des Sprengstoffangriffs auf einen Verstoß gegen das Versammlungsgesetz und stellte auch dieses Verfahren nach kurzer Zeit ein.

Ähnlich falsch oder irreführend sind auch alle übrigen gespeicherten „Delikte“, die teilweise bis in das Jahr 2002 zurückreichen. Darunter befinden sich Einträge über angebliche Verstöße gegen das Urheberrecht: So hatte sich ein Polizist in Coburg beschwert, dass Kietzmann bei einer Demonstration eine Gruppe von Polizisten fotografiert hatte. Das ist zwar legal, führt aber immer wieder zu Anzeigen, die – wie auch bei Kietzmann – in der Regel zügig eingestellt werden. Trotzdem finden sich solche Beschuldigungen auch nach acht Jahren noch in den Datenbanken des BKA.

Die einzige Verurteilung im Leben des Fotografen liegt bereits 14 Jahre zurück: Für einen Verstoß gegen das Versammlungsgesetz wurde Kietzmann im Januar 2003 zu einer Geldstrafe von 320 Euro verurteilt. Es ging um die Teilnahme an einem gewaltfreien Studentenprotest. In den Datenbanken der Polizei soll dieses Bagatelldelikt aus Jugendzeiten allerdings noch mindestens bis Juli 2021 gespeichert bleiben.

Die Akte Kietzmann ist die umfangreichste der zehn BKA-Auskünfte, die das ARD-Hauptstadtstudio auswertete. Doch auch in allen anderen finden sich zahlreiche Einträge, die entweder offensichtlich falsch sind oder von Juristen für eindeutig rechtswidrig gehalten werden.

Im Fall des Stuttgarter Online-Journalisten Alfred Denzinger ist ein sieben Jahre alter Datensatz wegen „Beleidigung“ aufgeführt, der auf die Anzeige eines vorbestraften Rechtsextremisten zurückgeht. Im Laufe des Ermittlungsverfahrens hatte sich schnell herausgestellt, dass nicht der Journalist eine Straftat begangen hatte, sondern der Rechtsextremist und ein Mittäter eine friedliche Mahnwache einer Schorndorfer Bürgerinitiative tätlich angegriffen hatten. Beide wurden dafür rechtskräftig zu Haftstrafen verurteilt, die Anzeige gegen Denzinger zurückgezogen. In der Verbunddatei des BKA soll der Eintrag noch bis Februar 2020 gespeichert bleiben.

Der in der Praxis nie zu einer Anklage führende Vorwurf eines unerlaubten Fotografierens von Polizisten findet sich gleich in mehreren Einträgen als „politisch motivierte Kriminalität“, wie das vermeintliche Delikt „Verstoß gegen das Versammlungsgesetz“. In all diesen Fällen ging es in Wirklichkeit nur darum, dass bei Demonstrationen auch die Personalien von Journalisten kontrolliert wurden.

An den Beispielen zeigt sich ein Muster, das weit über den Fall der entzogenen Akkreditierungen hinaus reicht. Um dieses zu konkretisieren, sollen die Fälle der Behörde der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) vorgelegt werden. DatenschützerInnen warnen seit Jahren, dass von der Polizei gespeicherte Daten erhebliche Nachteile für die berufliche und private Existenz von Bürgern haben können. Frühere Überprüfungen deuten darauf hin, dass sich das Ausmaß und die Qualität der fehlerhaften und rechtswidrigen Datenspeicherungen nicht geändert hat.

So hatte der damalige BfDI Peter Schaar im Jahre 2012 die Datenbank „PMK-links Z“, in der politisch motivierte Kriminelle gespeichert werden, überprüft und dabei viele Rechtsverstöße festgestellt. Das BKA löschte in der Folge rund 90% der Einträge. Statt 3819 Personen im März 2012 waren im Juli 2015 nur noch 331 Personen gespeichert. Schaar: „Spätestens zu diesem Zeitpunkt war klar, dass die Polizei mit den Kriterien, die eine Speicherung rechtfertigen, zu großzügig umgegangen war.“

Eine ähnlich hohe Quote rechtswidriger Einträge dürfte auch für andere Dateien gelten, wobei es bei den Fallzahlen um ganz andere Größenordnungen geht. Nach Auskunft des Bundesinnenministeriums (BMI) sind in der Datei „Innere Sicherheit“ im Herbst 2017 109.625 Personen und 1.153.351 Datensätzen zu Delikten gespeichert. Das ist das 27-fache der 41.549 politisch motivierten Straftaten, die laut Kriminalstatistik im Jahre 2016 insgesamt begangen wurden. Die 2012 vom BKA angekündigten Korrekturen an der überzogenen Speicherungspraxis waren anscheinend nicht nachhaltig. Betroffen sind sämtliche Kategorien von Straftaten. Von den in der „Fallgruppe Rauschgift“ gespeicherten mehr als 473.000 Personen mit Millionen von Datensätzen liegen mehr als die Hälfte der Einträge mehr als zehn Jahre zurück. Ein Blick in die Polizeistatistik zeigt, dass weit über die Hälfte dieser Menschen irgendwann einmal mit geringen Mengen Cannabis in Verbindung gebracht wurden. Derartiges führt in der Regel nicht zu einer Anklage, wohl aber systematisch zu langjährigen Speicherungen in den Datenbanken des BKAs, ohne dass die meisten Betroffenen das ahnen.

Eine Erklärung der hohen Zahl rechtswidrig gespeicherter Datensätze gibt die offene Formulierung des § 8 des Gesetzes über das Bundeskriminalamt (BKAG). Danach ist die Speicherung von Ermittlungen auch zulässig, wenn diese nicht zu einer Verurteilung vor Gericht geführt haben. Gefordert wird lediglich in jedem Einzelfall eine „Negativprognose“: Dabei müsste konkret begründet werden, warum von der Person auch in Zukunft Straftaten zu erwarten sind und die Speicherung früherer Ermittlungen deshalb nötig sei. Die Datenschutzaufsichtsbehörden kritisieren allerdings seit Jahren, dass diese Datensätze auch ohne eine solche „Negativprognose“ über Jahre gespeichert bleiben. So führte der Datenschutzbericht 2017, der wenige Wochen vor dem G20-Gipfel kaum beachtet veröffentlicht wurde, aus: „Das kehrt die Unschuldsvermutung gegen die sonst geltenden Prinzipien um und widerspricht der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und des Bundesverfassungsgerichts.“ Im Gesetz müsse dagegen künftig eindeutig geregelt werden, dass jeder Freispruch automatisch zur Löschung aller entsprechenden Datensätze führen müsse.

Peter Schaar weist darauf hin, dass die Masse an Daten die Ermittlungsarbeit der Polizei nicht erleichtere, sondern behin-

dert: „Das Beispiel des Attentäters vom Berliner Breitscheidplatz belegt, dass Sicherheitsbehörden angesichts immer zahlreicherer Datensätze den Überblick verloren haben und letztlich zu falschen Bewertungen gekommen sind. Weniger wäre mehr.“ Im Ergebnis nütze es dem Rechtsstaat und stärke zugleich die Polizeiarbeit, wenn man sich auf relevante Daten beschränke.

Der frühere Bundesverfassungsrichter Wolfgang Hoffmann-Riem, der die unrechtmäßige Speicherung von Daten schon mehrfach als „skandalös“ bezeichnet hatte, forderte eine umfassende Aufklärung, die deutlich über den Fall der G20-Akkreditierungen hinaus reicht: „Es geht um drei unterschiedliche Probleme: Wann muss eine Eintragung, selbst wenn sie anfänglich rechtmäßig war, aus allen Dateien entfernt werden, in die sie inzwischen gelangt ist? Zweitens: Reicht eine Eintragung als solche, um bei dem Betroffenen eine Gefahr für die öffentliche Sicherheit begründen zu können? Drittens: Die Polizei muss bei der Entscheidung über einen Eingriff gegen einen Journalisten berücksichtigen, dass Journalisten bei ihrer Arbeit der besondere Schutz der Medienfreiheit zusteht. Auf allen drei Ebenen scheinen Fehler begangen worden zu sein. Hier muss dringend für rechtsstaatliche Klarheit gesorgt werden.“

Innenexperte Konstantin von Notz von den Grünen im Bundestag erklärte: „Ganz offensichtlich wurden die Akkreditierungen in einer relevanten Anzahl von Fällen auf Grundlage falscher Tatsachen entzogen. Das ist für die Bundesregierung nicht nur maximal peinlich, es stellt vor allem einen erheblichen Eingriff in die Pressefreiheit dar.“ Von Notz sieht vor allem den Bundesinnenminister in der Verantwortung, der die Warnungen der Datenschützer über Jahre in den Wind geschlagen habe: „Seit Jahren dokumentiert das unionsgeführte Ministerium, wie egal ihm der Datenschutz ist. Der Datenschutz schützt aber keine Daten, sondern unsere Menschenwürde und Privatsphäre.“ Im vorliegenden Fall erkenne man gut, wie abgründig und willkürlich staatliches Handeln werden kann, wenn es auf rechtswidrigen, schlecht kontrollierbaren und schlampig geführten Dateien beruhe. Das Versagen müsse vom Parlament aufgeklärt werden und spielt auf einen möglichen Untersuchungsausschuss an: „Sollte die Bundesregierung mauern, müssen wir schärfere parlamentarische Instrumente ins Auge fassen.“ SPD-Fraktionschef Thomas Oppermann kritisierte, das BKA speichere offenbar „wahllos Informationen über unschuldige Bürger“. Der CSU-Innenpolitiker Stephan Mayer forderte „sehr akribische und sorgfältige“ Prüfungen. SPD-Noch-Justizminister Heiko Maas verlangte „umfassende Aufklärung“.

Das Bundesinnenministerium (BMI) räumte zwischenzeitlich ein, dass der Entzug der Akkreditierung in mindestens fünf der insgesamt 32 Fälle eine falsche Grundlage gehabt hat. Als für das BKA zuständige Behörde bedauerte es das und sagte zu, alle betroffenen Datensätze neu zu überprüfen. Die stellvertretende Regierungssprecherin Ulrike Demmer hatte zuvor erklärt, man werde sich bei allen Betroffenen offiziell entschuldigen. Verärgert zeigte sich das BMI über die Reaktionen der SPD. Alle Fehler in den BKA-Speicherungen gingen auf fehlerhafte Informationen von Landesbehörden zurück, darunter auch SPD-geführte. Ob Verfahren eingestellt oder mit einem Freispruch geendet hätten, werde zu oft nicht an die Polizeien und erst recht nicht an das BKA weitergeleitet (Henze, Millionen rechtswidrige Daten in BKA-Datei? www.tagesschau.de 30.08.2017; Braun, Falsch gespeichert, SZ 01.09.2017, 6).

Bund

Türken fürchten Asylanhörungen wegen möglicher Datenweitergabe

Türkische Asylsuchende erheben schwere Vorwürfe gegen Mitarbeitende des Bundesamtes für Migration und Flüchtlinge (BAMF): In mehreren Fällen seien Betroffene kurz nach Anhörungen beim BAMF oder bei Ausländerbehörden in türkischen Medien mit sehr spezifischen Informationen, die mit großer Wahrscheinlichkeit aus der Anhörung stammten, als „Terroristen“ diffamiert worden. Von den Zeitungen und Fernsehsendern, die dem türkischen Präsidenten Recep Tayyip Erdogan nahestehen, wurde der genaue Aufenthaltsort der Asylsuchenden genannt; teils wurde explizit auf ihr Asylverfahren Bezug genommen. Die Betroffenen gaben an, zuvor ihre Identität streng geheim gehalten zu haben. Sie verdächtigen daher Menschen aus dem BAMF-Zusammenhang, die Informationen, evtl. über den türkischen Geheimdienst, an die türkischen Medien weitergegeben zu haben. In mindestens zwei Fällen ermitteln nun Staatsschutzabteilungen der Polizei.

Ein kurdischer Journalist und Anhänger des Erdogan-Gegners Fethullah Gülen, der in der Türkei zum Staatsfeind erklärt worden war, hatte sich monatelang in Deutschland versteckt; nur engste Vertraute kannten seinen Aufenthaltsort. Eine Stunde nach seinem BAMF-Termin tummelten sich deutsche Erdogan-Fans auf seinem Twitter-Account; fünf Tage später bezichtigte ihn ein türkischer Publizist in einem Tweet als Mitglied der verbotenen Kurdenpartei PKK und der „Terrororganisation Fetö“, wie Erdogan die Gülen-Bewegung bezeichnet, und nannte die deutsche Stadt, in der er lebt. Der Betroffene vermutet, dass die Information über den türkischen Dolmetscher im BAMF leakte. Unter den Sachbearbeitenden, Dolmetschern und Sicherheitsleuten des BAMF sowie auch bei Ausländerbehörden sind einige türkischstämmig. Eine ähnliche Geschichte berichtete ein Mann, der vor dem Putschversuch in der Türkei ein hochrangiger Beamter war und im Februar 2017 nach Deutschland floh. Bei einem Termin bei der Ausländerbehörde wurde ein türkischer Sicherheitsmann zum Übersetzen hinzugezogen, weil kein Dolmetscher zur Verfügung stand. Kurz danach strahlte ein türkischer Fernsehsender einen Beitrag über den Mann aus, zeigte ihn mit Bildern beim Einkaufen und nannte den Ort seines jetzigen Aufenthalts. Er meinte: Deutschland hat eine große türkische Gemeinschaft, da ist die Chance, dass Spitzel darunter sind, ebenfalls groß.“ Andere Asylsuchende berichteten, dass ihre Anhörung als Verhör geführt wurde, in dem sie sich immer wieder nicht mit Fragen, sondern mit Vorwürfen konfrontiert sahen.

Das BAMF teilte mit, es sei kein Fall bekannt, in dem Mitarbeitende Informationen über Asylsuchende an türkische Stellen weitergegeben hätten. Allerdings trennte sich die Behörde nach eigenen

Angaben seit Jahresbeginn in 15 Fällen von freiberuflichen Dolmetschern „vor allem aufgrund von Verletzungen der Neutralitätspflicht“. Einer hatte islamische Anschläge gebilligt; ein anderer entpuppte sich als Antisemit. Zuletzt war ein aus Vietnam stammender langjähriger Mitarbeiter der BAMF-Außenstelle Jena entlassen worden, weil sich herausstellte, dass er bei Facebook gegen vietnamesische Oppositionelle gehetzt hatte, die in Deutschland leben. Mit mehreren Hundert freiberuflichen Dolmetschern hat das BAMF im Jahr 2017 seine Zusammenarbeit beendet, weil sie nicht mehr gebraucht würden. Das BAMF kündigte eine „sehr genaue und umfassende Untersuchung“ an. Die von der Presse thematisierten Fälle hätten aber nicht nachvollzogen werden können. Man habe festgestellt, „dass es keine zentralen Beschwerden zu diesen Sachverhalten geben hat“.

Grünen-Chef Cem Özdemir forderte, die Sicherheitsüberprüfung für Dolmetscher zu verschärfen: „Jeder, der für die Sicherheit unseres Landes arbeitet, muss sich loyal zu Deutschland und keinem anderen Land zeigen“.

Nach dem Putschversuch im Juli 2016 haben zahlreiche türkische Militärangehörige, aber auch Diplomaten Zuflucht in anderen Staaten Europas gesucht. Bis Mitte September 2017 hatten in Deutschland mehr als 600 ranghohe türkische Staatsbeamte um Asyl gebeten. Gemäß einer Sprecherin des Bundesinnenministeriums haben 255 Inhaber türkischer Diplomatenpässe sowie 383 Besitzer eines türkischen Dienstpasses Asylanträge gestellt. Die türkischen Asylsuchenden haben Angst, dass der Arm des türkischen Geheimdienstes bis nach Deutschland reicht und sie nicht nur beobachtet, sondern diffamiert, beleidigt und körperlich angegriffen werden.

Die Regierung in Ankara kritisiert es scharf, dass die Bundesregierung türkischen Soldaten Asyl gewährt. Sie wirft ihnen Verbindungen zu dem in den USA im Exil lebenden islamischen Prediger Fethullah Gülen vor. Gülen und seine Anhänger macht die türkische Regierung für den gescheiterten Putschversuch verantwortlich (Spitzel-Verdacht bei Ausländerbehörden, SZ 16.10.2017, 9; Türkei Bamf-Mitarbeiter sollen türkische Asylbewerber bespitzelt haben, www.tagesspiegel.de 14.10.2017; Knobbe/Wiedmann-Schmidt, Spitzeln im Amt, Der Spiegel 42/2017, 47).

Bund

LSVD: Nach Schwulenheirat Diskriminierung im Heimatland verhindern!

Seit dem 01.10.2017 können in Deutschland erstmals homosexuelle Paare – so wie bisher Mann und Frau – heiraten. Was für viele schwule und lesbischen Paare ein großes Glück ist, kann sich für solche, bei denen eine PartnerIn aus einem Land stammt, in dem Homosexuelle diskriminiert werden, als Handicap erweisen, da die Änderung ihres Personenstands den Herkunftsländern mitgeteilt wird. Die Weltkarte der International Lesbian and Gay Association (ILGA) dokumentiert den rechtlichen Status von Lesben, Schwulen, Bi- und Intersexuellen. Demnach besteht in 76 Staaten ein homophobes Strafrecht. In sieben Staaten (Iran, Jemen, Mauretanien, Saudi-Arabien, Teile von Nigeria und Somalia) sind Schwule von der Todesstrafe bedroht. In 22 asiatischen Staaten werden Homosexuelle strafrechtlich verfolgt. Auch in 10 karibischen Inselstaaten sind homosexuelle Handlungen strafbar.

Am 01.11.2017 trat ein Personenstands-Änderungsgesetz in Kraft. Die VertreterInnen des Lesben- und Schwulenverbands Deutschland (LSVD) haben erfolgreich darauf gedrungen, dass ausländischen Vertretungen nicht Auskunft aus Personenstandsregistern gegeben werden darf, wenn die Angehörigen dieses Staates in homosexuellen Lebenspartnerschaften leben. Damit soll verhindert werden, dass Schwule und Lesben in ihren Herkunftsländern bei Familienbesuchen entwürdigt und bloßgestellt werden, amtsärztlichen Untersuchungen über sich ergehen lassen müssen oder inhaftiert werden.

Manfred Bruns, ehemaliger Bundesanwalt beim Bundesgerichtshof und LSVD-Fürsprecher: „Während des Gesetzgebungsverfahrens war nicht abzusehen, dass es demnächst auch gleichgeschlechtliche Ehen geben würde.“ In einem Brief an das Bundesinnenministerium fordert er nun, dass das Gesetz nachgebessert wird: „Die Standesämter müssen angewiesen werden, in der Zwischenzeit auch über gleichgeschlechtlich verheiratete Ausländer keine Auskunft zu erteilen.“ Zwar heißt es jetzt schon im neuen Gesetz: „Ob Mitteilungen an ausländische Stellen aufgrund zwischenstaatlicher Vereinbarungen erfolgen können, ist unter Berücksichtigung der unterschiedlichen Kulturkreise im Einzelfall zu prüfen.“ Dies bezieht sich aber nur auf vertraglich vorgesehene automatische Datenübermittlungen. Die Erteilung von Personenstandsurkunden und Auskünfte aus einem Personenstandsregister werden damit jedoch noch nicht angesprochen (Heidenreich, Geheimhaltung statt Glückwünsche, SZ 09.10.2017, 5).

Bund

Jobcenter meldet an Verfassungsschutz

Aus einer Antwort des Bundessozialministeriums auf eine Anfrage der Linken im Bundestag geht hervor, dass in den letzten zwei Jahren in 11 Fällen von Jobcentern Informationen an die jeweils zuständigen Landesämter für Verfassungsschutz weitergegeben wurden, wenn bei Arbeitslosen ein Extremismusverdacht bestand. Die Verdachtsmomente bezogen sich in vier Fällen auf Islamismus, in drei Fällen auf die „Reichsbürgerbewegung“ und in je einem Fall auf „Terror“ und „Gefährdung“ (Kieler Nachrichten, Jobcenter melden Verdächtige, 23.09.2017, 4).

Bund

Frauke Petry kopierte AfD-Kontaktdaten

Der Datenschutzbeauftragte der Rechtsaußen-Partei Alternative für Deutschland (AfD) wirft der damaligen AfD-Bundeschefin Frauke Petry vor, sich wenige Tage vor der Bundestagswahl am 24.09.2017 einen großen Datensatz aus der Mitgliederkartei der Partei verschafft zu haben. Sie habe am Abend des 15.09.2017 mehr als 116.000 Kontaktdatensätze aufgerufen und große Mengen kopiert. Dies sei rechtswidrig, weshalb

sie die Daten löschen müsse. Petry hatte am Tag nach der Wahl angekündigt, nicht der AfD-Fraktion anzugehören und war dann am 29.09. aus der Partei ausgetreten. Die verbleibende AfD-Führung befürchtet, dass Petry eine neue Partei gründen und die Daten nutzen möchte, um Parteigänger anzuwerben. Petry bestätigte dem AfD-Datenschutzbeauftragten, sie habe sich einen Zugang zur Datenbank geben lassen, aber nur nachdem „mein persönlicher Zugang ohne Information offenbar Wochen vorher massiv und ohne Begründung eingeschränkt“ worden sei. Sie habe sich nur „über den aktuellen Mitgliederstand informiert“ und die Daten anschließend gelöscht (Der Spiegel 41/2017, 23).

Baden-Württemberg

Polizeigesetz mit Quellen-TKÜ und „intelligenter“ Videoüberwachung

Die grün-schwarze Landesregierung Baden-Württembergs hat einen Entwurf für ein neues Polizeigesetz vorgelegt, der am 10.10.2017 erstmals im Stuttgarter Landtag diskutiert wurde. Der Entwurf stieß bei DatenschützerInnen und RichterInnen auf grundlegende Kritik. Er sieht die Ausweitung von Video- und Telekommunikationsüberwachung vor, die Einführung des Staatstrojaners und der elektronischen Fußfessel, ein Kontaktverbot für „Gefährder“ und ein polizeiliches Alkoholverbot auf öffentlichen Plätzen. Spezialeinheiten der Polizei sollen mit Sprengstoff und Handgranaten ausgerüstet werden, die sie auch gegen Menschen einsetzen dürfen.

Der Polizei soll künftig erlaubt sein, „intelligente“ Videoüberwachung einzusetzen. Dadurch würde, so der Entwurf, die Eingriffstiefe verringert. Dem widerspricht der baden-württembergische Landesbeauftragte für Datenschutz und Informationsfreiheit (LfDI) Stefan Brink unter Verweis auf ein Urteil des Bundesverfassungsgerichts (1 BvR 518/02) zur Rasterfahndung, wonach automatisierte Operationen herkömmliche Verfahren mit „einer bislang unbekannten Durchschlagskraft versehen“ können. Die Aussage der Landesregierung, Verhaltensmuster wie etwa Bewegungsabläufe oder Gruppenbildung würden nicht anhand personenbezogener Merkmale automatisiert ausgewertet, hält Brink für „schlichtweg nicht nachvollziehbar“. Verhaltensweisen einer Person gehörten zu den persönlichen Verhältnissen einer Person – und das Erkennen von Verhaltensmustern sei ja das Ziel der intelligenten Videoüberwachung.

Brink kritisiert vor allem, dass BürgerInnen sich nicht sicher sein können, welche ihrer Verhaltensweisen vom Algorithmus als polizeilich relevant gedeutet werden. „Schnelles Laufen, etwa an einer Haltestelle, freundschaftliches Schulterklopfen, das Unterhaken des Ehepartners oder harmlose Raufereien Jugendlicher können schnell dazu führen, dass Betroffene sich polizeilichen Maßnahmen ausgesetzt sehen.“ Automatisch ausgewertet werden dürften daher nur solche Verhaltensmuster, die eine „konkrete Wahrscheinlichkeit begründen, dass es in absehbarer Zeit zu einer Straftat kommt“. Die Polizei müsse etwa mit Hinweisen und Piktogrammen bekannt machen, welche Verhaltensweisen als relevant eingestuft werden. Brink verlangt außerdem, intelligente Videoüberwachung nur unter den vorgesehenen „räumlichen und inhaltlichen Voraussetzungen“ einzusetzen. Die Landesregierung sieht lediglich eine vorläufige Eingrenzung vor. Das System dürfe nur die Geschehensabläufe übertragen und aufzeichnen, die von ihm als polizeilich relevant erkannt werden.

Der baden-württembergische Richterverein argumentiert in seiner Stellungnahme ähnlich. Es „dürfte nicht ausreichen“, dass der Verkäufer einer Software diese für „intelligent“ halte: „Wenn nicht der Eindruck entstehen soll, dass die aktuellen Terroraktivitäten benutzt werden sollen, polizeiliche Befugnisse insgesamt auszuweiten, sollte dringend ein Nachweis der Geeignetheit geführt werden.“

Die baden-württembergische Landesregierung will zudem die Quellen-Telekommunikationsüberwachung einführen. Diese ist laut Bundesverfassungsgericht dann rechtmäßig, wenn sie ausschließlich der Terrorismusabwehr dient. Anders als das BKA-Gesetz beschränkt sich der Entwurf in Baden-Württemberg nicht darauf, weshalb Staatstrojaner auch schon bei einer Körperverletzung zum Einsatz kommen könnten. Das verstößt nach Brinks Meinung klar gegen den Verhältnismäßigkeitsgrundsatz. Er weist darauf hin, dass Betroffene über keine „hinreichende Möglichkeit“ verfügten, die Abhörmaßnahme gerichtlich überprüfen zu lassen. Betroffene würden gegenwärtig nur ausnahmsweise benachrichtigt. Das müsse der Gesetzgeber ändern.

Der Entwurf enthält weitere brisante Regelungsvorschläge. Unter anderem soll Spezialeinsatzkommandos der Polizei der Einsatz von Explosivmitteln wie Handgranaten erlaubt werden. Der grüne Ministerpräsident Winfried Kretschmann hatte gegenüber der Presse erklärt: „Wir gehen an die Grenze des verfassungsmäßig Machbaren.“ Dies ist, so Brink, mit einem doppelten Risiko verbunden: „Er überantwortet die Letztentscheidung zu sicherheitspolitischen Fragen dem Verfassungsgericht und er läuft Gefahr, Anlass und Zweck der Sicherheitsnovelle aus den Augen zu verlieren.“ Keines der neuen Sicherheitsinstrumente habe bislang seine Wirksamkeit unter Beweis gestellt.

Brink fordert daher eine parlamentarische wie auch gerichtliche Evaluierung dieser Instrumente noch in der laufenden Legislaturperiode. Der Richterverein kommt ebenfalls zu dem Fazit, dass der Gesetzesentwurf Mittel aufführt, „deren Geeignetheit für die Bekämpfung dieser Bedrohungen nicht belegt ist“. Er enthalte zudem „Formulierungen für die Voraussetzungen zu Überwachungsmöglichkeiten, die zu weitgehend oder unzureichend präzise formuliert sind“ (Schulzki-Haddouti, Harsche Kritik an grün-schwarzen Überwachungsplänen, www.heise.de 12.10.2017; Reuter, Baden-Württemberg: Datenschutzbeauftragter kritisiert grün-schwarzes Anti-Terror-Paket, netzpolitik.org 10.10.2017).

Bayern

LDA beanstandet Facebooks Custom Audience

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) stellte im Rahmen einer Prüfung von 40 bayerischen Unternehmen fest, dass „Facebook Custom Audience“ von Unternehmen oftmals rechtswidrig eingesetzt wird. Es prüfte den Einsatz von zwei Varianten des zielgruppenorientierten Werbetools.

BayLDA-Präsident Thomas Kranig kam dabei zu dem Ergebnis: „Es findet eine systematische Durchleuchtung der Nutzer durch die Algorithmen von Facebooks Künstlicher Intelligenz statt." Selbst Nutzende, die regelmäßig Cookies löschen, Datenschutzeinstellungen nutzen oder sogar kein Mitglied in sozialen Netzwerken sind, würden verfolgt. Adressat von Anordnungen bzw. Bußgeldbescheiden wäre dann nicht Facebook, das sind vielmehr die jeweiligen Unternehmen, die das Werbemittel unzulässig einsetzen.

Facebook bietet an, sein Werbetool über ein Kundenlisten- und ein Pixel-Verfahren zu nutzen. Beim Pixel-Verfahren bindet das Unternehmen ein Facebook-Pixel auf seiner Website ein, um das Online-Verhalten der Nutzenden über Facebook nachvollziehen zu können. Über das Pixel werden Kundendaten wie Name und Mail-Adresse an Facebook übermittelt und mit Tracking-Daten angereichert. Das Unternehmen erfährt so beispielsweise, welches Produkt eine NutzerIn in den Warenkorb gelegt hat, bevor sie die Bestellung abgebrochen hat. Das Unternehmen kann dann über Facebook die NutzerIn mit dem in den Warenkorb gelegten Produkt bewerben und zum Webshop zurückführen, damit sie die Bestellung doch noch abschließt.

Die Prüfung des BayLDA ergab, dass die Nutzenden beim Pixel-Verfahren „oftmals" nicht oder nicht vollständig informiert werden und kein Opt-Out-Verfahren nutzen können. Mitunter wurde ein Opt-Out auch nicht technisch korrekt umgesetzt, sodass weiterhin Online-Daten an Facebook übertragen wurden. Damit verstießen die Unternehmen jeweils gegen geltendes Datenschutzrecht. Überdies weist das BayLDA darauf hin, dass mit dem Pixel auch Daten von Nicht-Facebook-NutzerInnen erhoben oder Nutzer erfasst werden, die während des Besuchs einer Webseite nicht bei Facebook eingeloggt sind. Damit würden auch Webseiten-BesucherInnen über Facebook verfolgt, die bewusst die Speicherung von Third-Party-Cookies unterbinden. Daher müssten die Unternehmen „vorab" eine informierte Einwilligungserklärung von allen Webseiten-Besuchern einholen.

Ein Unternehmen kann Facebooks Werbetool auch über eine Kundenliste nutzen, die es über sein Facebook-Konto hochlädt. Zuvor werden die Kundendaten mit einem Hash-Verfahren in eine feste Zeichenkette umgewandelt. Facebook gleicht diese Liste dann mit allen Facebook-Nutzenden ab. Das Unternehmen startet daraufhin seine Werbekampagne für die KundInnen, die auf Facebook sind, und wählt hierfür eine Zielgruppe mit bestimmten Merkmalen wie Alter oder Interessen aus.

Das BayLDA hält das verwendete Hashverfahren für nicht geeignet, anonyme Zeichenfolgen zu generieren. Die Hash-Werte konnten mit geringem Aufwand zurückgerechnet werden. Das BayLDA meint daher, dass die Unternehmen personenbezogene Daten ohne Einwilligung der Betroffenen rechtswidrig übermittelt haben.

Kranig stellt fest, dass den geprüften Unternehmen der Rechtsrahmen häufig „völlig unklar" war. Überdies könnten Unternehmen, die nicht wissen, wie solche Werbetools funktionieren, ihre Nutzenden auch nicht richtig über deren Einsatz informieren. Kranig: „Wer das nicht kann, darf eben solche Tools nicht einsetzen." Vorerst hat Kranig keine Sanktionen verhängt. Er stellt jedoch den Unternehmen „allgemeine Hinweise und Anforderungen" zum Einsatz von Facebook Custom Audience zur Verfügung, die sie zu beachten haben und kündigte an, die Prüfung „zu gegebener Zeit" fortzusetzen. (Schulzki-Haddouti, Datenschützer: Unternehmen setzen gezielte Werbung von Facebook oft rechtswidrig ein, www.heise.de 05.10.2017).

Berlin

Datenschutzbeschwerden über Bringdienste

In der Dienststelle der Berliner Beauftragten für Datenschutz (BlnBDI) gehen seit Mitte 2015 vermehrt Beschwerden über Essensbringdienste wie Delivery Hero (Lieferheld, Foodora, Pizza.de) ein. Bis August 2017 waren 14 Anzeigen aktenkundig. Die KundInnen rügten meist, dass ihr Account nicht gelöscht wurde oder dass sie hierfür einen Identitätsnachweis zusenden sollten. Acht Fälle wurden gemäß einer Specherin der BlnBDI ohne Sanktionen wieder abgeschlossen, nachdem die Anbieter kooperiert hatten; die anderen werden noch bearbeitet. Ende Juni 2017 hatte Delivery Hero den größten Börsengang des Jahres hingelegt. Mit den frischen Millionen will die Firma den Kampf gegen den niederländischen Dauer-Konkurrenten Takeaway (Lieferando) endgültig für sich entscheiden. Die beiden Kontrahenten ringen um Kundschaft und Restaurants. Beide betreiben einen extrem hohen Marketingaufwand, allein Delivery Hero gab 2016 für TV- und Radiowerbung 106 Mio. € aus. Kundendaten sind für die Lieferfirmen von großer Bedeutung.

Delivery Hero hat wie seine deutschen Tochterunternehmen seinen Sitz in Berlin, weshalb die aufkommenden Datenschutzklagen bei der Berliner Behörde auflaufen. Auch im „Düsseldorfer Kreis", einer Konferenz von 17 deutschen Datenschutzbehörden, waren die Bringdienste inzwischen Thema. Die BlnBDI schlug dort eine bundesweite „koordinierte Prüfaktion bei Essenslieferdiensten" vor, um diese „für datenschutzrechtliche Belange zu sensibilisieren" (Kunden beschweren sich über Delivery Hero, www.spiegel.de 26.08.2017).

Sachsen

Massenhafte Abhöraktion u. a. gegen Berufsgeheimnisträger

Bei Ermittlungen im Umfeld des sächsischen Fußballvereins BSG Chemie Leipzig wurden auch Gespräche mit JournalistInnen, ÄrztInnen und RechtsanwältInnen abgehört und gespeichert. Die Generalstaatsanwaltschaft des „Freistaats Sachsen" hatte gegen 14 Personen aus dem von der Polizei als politisch links verorteten Umfeld des Fußballvereins BSG Chemie Leipzig wegen des Verdachts auf Bildung einer kriminellen Vereinigung ermittelt. Im Rahmen dieses Ermittlungsverfahrens waren Gespräche von mindestens drei Journalisten abgehört und jahrelang gespeichert worden. In mindestens einem Fall waren Gesprächsinhalte im Herbst 2017 immer noch gespeichert;

in den anderen Fällen waren die Daten erst kurz vor Ende der Ermittlungen im September 2016 gelöscht worden. Trotz der direkten Betroffenheit von Berufsgeheimnisträgern wurden die Daten nicht umgehend gelöscht. Zudem hätten die JournalistInnen nach Einstellung des Verfahrens über die Abhörmaßnahmen von der Generalstaatsanwaltschaft Dresden informiert werden müssen. Die drei Betroffenen versicherten im Sommer 2017, dass dies in keinem der Fälle geschehen sei. Neben den Beschuldigten waren mehr als 200 Personen abgehört worden, die Protokolle Zehntausender Gespräche füllten am Ende 80 Aktenordner. Trotz dieses enormen Aufwandes wurden die Ermittlungen im Oktober 2016 aus Mangel an Beweisen eingestellt.

Im Oktober 2017 ist durch den Grünen-Landtagsabgeordneten Valentin Lippmann herausgekommen, dass entgegen vorheriger Mitteilungen der Generalstaatsanwaltschaft „mindestens neun Journalisten, zehn Rechtsanwälte und drei Ärzte als Dritte von den Überwachungsmaßnahmen“ betroffen gewesen sind. Insgesamt sind demnach mehr als 360 Anrufe und SMS mit Berufsgeheimnisträgern von den Behörden abgehört und protokolliert worden. Ein Journalist der Leipziger Volkszeitung wurde allein 130mal belauscht, als er mit Vertretern von Chemie Leipzig telefonierte. Lippmann kritisierte angesichts der neuen Erkenntnisse die „Salamitaktik“ von Justizminister Sebastian Gemkow (CDU) und stellte die Prioritäten der Sicherheitsbehörden in Frage. So habe es enorme Ressourcen gegeben, die linke Szene auszukundschaften, obwohl Sachsen bekanntlich ganz andere Probleme habe (Pollmer, Lauschrausch, SZ 19.10.2017, 23).

Datenschutznachrichten aus dem Ausland

Weltweit

Google rüstet Kameras für Street-View auf

Acht Jahre nach dem Start von Google Street-View rüstet die Firma Kamera-Fahrzeuge auf, mit welchen die Straßen der Welt fotografiert werden. Die bisher verwendeten Kameras sind nicht mehr die allerneuesten und von Anfang an im Einsatz. Manche Straßenansicht wirkt so neblig-flau. Seit August 2017 sind die ersten verbesserten Kameras auf den Straßen unterwegs, die schärfere Bilder mit lebhafteren Farben liefern und die Auswertbarkeit verbessern, um mit extrahierten Daten Googles Datenbanken zu befüllen. Die höher aufgelösten Bilder enthalten mehr erkennbare Daten wie die Öffnungszeiten von Geschäften, sofern diese außen vermerkt sind.

Google analysiert die Fotos mit künstlicher Intelligenz und neuronalen Netzen und versucht, möglichst aussagekräftige Informationen herauszulesen, z. B. neu eröffnete Geschäfte zu erkennen. Die Algorithmen erkennen Straßennamen und Hausnummern und platzieren die erfassten Adressen auf einer Karte. Die ausgewerteten Daten nutzt Google dann für seine Dienste, nicht nur Google Maps, sondern z. B. auch für die Fakten-Datenbank „Knowledge Graph“ und ergänzt Google-Suchergebnisse um Meta-Informationen.

Google meint, ihre NutzerInnen verlangten immer mehr und komplexere Informationen. Die Suchanfragen würden immer schwieriger und anspruchsvoller; statt nur eine Adresse bei Google Maps einzugeben, schrieben die Suchenden ausformulierte Anfragen wie: „Welches vegane Restaurant in der Südstadt hat jetzt noch geöffnet?“ Bei der Beantwortung solcher kontextbezogenen Fragen sollen die besseren Fotos helfen. Bald könne Maps sogar Anfragen wie „Was ist der Name des pinken Geschäfts neben der Kirche an der Ecke?“ beantworten.

Aus den Bildern von Street-View lassen sich viele Informationen ableiten. Ein Team von Stanford-Forschenden hat mit Street-View Details über das Einkommen und das Wahlverhalten einer Nachbarschaft herauszufinden versucht, indem sie die Autos, die auf den Bildern zu sehen sind, analysierten. Teure Marken wurden als Indiz für hohe Einkommen gewertet. Was die Privatsphäre in Street-View angeht, hat Google keine Bedenken. Jen Fitzpatrick, Chefin der Google-Maps-Sparte, erklärte, dass ihr kein Ort bekannt sei, wo es besondere Probleme gegeben habe.

Google macht auf den Street-View-Bildern weiterhin Gesichter und Nummernschilder automatisch unkenntlich. Als Street-View 2010 in Deutschland startete, löste der Dienst schon vor seinem Start heftige Reaktionen bei DatenschützerInnen aus. Diverse HausbesitzerInnen wollten daraufhin ihr Anwesen nicht im Internet sehen. Google macht seitdem auf Wunsch die Häuserfassaden unkenntlich. Insgesamt ist Deutschland verhältnismäßig schlecht abgedeckt (Berger, Google rüstet Street-View-Kameras auf, www.heise.de 07.09.2017).

Weltweit

Datenleck bei Accenture

Der weltweit agierenden Consulting-Firma Accenture ist ein schwerer Sicherheitspatzer passiert: Auf mindestens vier Servern in Amazons AWS-Cloud hatte das Unternehmen hunderte Gigabyte an vertraulichen Daten ohne Passwortschutz und größtenteils unverschlüsselt ins Netz gestellt. Das stellten Sicherheitsforschende der Fa. Upguard fest. Fremde hätten so Zugangsdaten zum Cloud-Service der Beraterfirma, Zertifikatsdaten, VPN-Schlüssel und allerhand Informationen über Kunden abgreifen können. Auch Accentures Masterkey für den AWS-Dienst sowie Zugangsdaten für Accounts der Firma bei Google und Microsofts Azure seien gefährdet

gewesen. Ein Großteil der Passwörter sei gehasht gewesen, doch rund 40.000 davon ließ man wohl komplett ungesichert. Darüber hinaus hätte man auch tiefe Einblicke in das Backend von Accentures Clouddienst bekommen, ebenso wie sensible Informationen über die Cloudmanagement-Plattform Enstratus. Der Sicherheitsforscher Chris Vickery, der das Leck entdeckt hatte, sprach von den „Schlüsseln für das Königreich".

Vickery hatte den unfreiwilligen Datenreichtum am 17.09.2017 bemerkt und nach kurzer Analyse Accenture benachrichtigt. Das Unternehmen sicherte die Server umgehend und erklärte, dass kein Risiko für die eigenen Kunden bestanden habe. Die Zugangsdaten seien zweieinhalb Jahre alt und für Nutzer eines inzwischen stillgelegten Systems gedacht gewesen. Einen Zugriff auf die ungesicherten Server habe man nicht feststellen können. Accenture rühmt sich damit, unter anderem zwei Drittel der 500 umsatzstärksten Unternehmen weltweit auf seiner Kundenliste zu haben. Sensible Daten einer solchen Consulting-Gesellschaft dürften also von großem Wert sein – und enormes Potenzial besitzen, um damit Schaden anzurichten (Kannenberg, Vertrauliche Daten von Accenture auf ungeschützten Webservern, www.heise.de 11.10.2017).

Frankreich

Ausnahmezustand wird teilweise Normalrecht

Im November 2017 endete der Ausnahmezustand in Frankreich. Fünf Mal war er verlängert worden; ausgerufen wurde er vom damaligen Präsidenten Francois Holland in der Nacht der Terroranschläge am 13.11.2015. Am 03.10.2017 verabschiedete nun das französische Parlament (Nationalversammlung) ein Gesetz zur „Verstärkung der Inneren Sicherheit und des Kampfes gegen den Terrorismus", das Elemente des Ausnahmezustands übernimmt. Mit 415 gegen 127 Stimmen bei 19 Enthaltungen fiel die Mehrheit deutlich zugunsten des neuen Gesetzes aus. Am 18.10.2017 wurde das Gesetz vom Senat bestätigt und kann damit in Kraft treten. Kurz vorher waren ein versuchter und vereitelter Anschlag sowie eine angeblich terroristisch motivierte Messerattacke bekannt geworden. Mitte September hatte Innenminister Gérard Collomb davon gesprochen, dass seit Januar dieses Jahres zwölf geplante Anschläge, wörtlich „Anschlagsprojekte", vereitelt wurden.

Das neue Gesetz für Innere Sicherheit und den Kampf gegen den Terrorismus war schon länger umstritten. Kritiker warfen dem Präsidenten Emmanuel Macron im Juni vor, dass er den „Ausnahmezustand in normales Recht überführen will". Es habe sich gezeigt, dass die frühere Regierung Regelungen des Ausnahmezustands auch als Mittel im Kampf gegen politische Militante nutzte und überstrapazierte: Sie untersagte Demonstrationen oder verbot AktivistInnen die Teilnahme, sonderte sie mit Präventivverboten aus. Die Kritik an diesen Befugnissen wurde teilweise vom Verfassungsrat geteilt, der die dazugehörigen Regelungen des Ausnahmezustands wegen Verstoß gegen das Aufenthaltsrecht von Personen und das Demonstrationsrecht aufhob. Diese weitgehenden Regelungen fehlen nun im neuen Gesetz.

Modifiziert wurde die ursprünglich geplante Regelung, wonach der Präfekt auch nach dem Ausnahmezustand weiter allein mit seiner Unterschrift Hausdurchsuchungen veranlassen kann, ohne dass dies richterlich bestätigt werden muss. Die Autorisierung durch einen Magistratsrichter für Hausdurchsuchungen ist nach dem neuen Gesetz wieder erforderlich. Der Präfekt hat aber künftig bessere Möglichkeiten, Orte der Religionsausübung, wie zum Beispiel Gebetsräume, umstandslos zu schließen. Er kann bei Terrorgefahr Sicherheitszonen einrichten, an denen jeder durchsucht werden kann, der sie betreten will. Der Terrorbekämpfung dient eine neue Task Force, die Macron im Élysée eingerichtet hat. Sie soll die diversen Geheimdienste des Landes koordinieren und sicherstellen, dass Informationen untereinander ausgetauscht werden.

Am Auffälligsten sind die Erweiterungen bei den Überwachungsbefugnissen, was u. a. von der Bürgerrechtsgruppe „La Quadratur du Net" scharf kritisiert wird. So ist eine heimliche Überwachung von Personen erlaubt, „die in gewohnheitsmäßige Beziehungen zu Personen oder Organisationen eintreten, die Ideen unterstützen, sie verbreiten oder ihnen anhängen, die zur Ausübung terroristischer Akte veranlassen oder diese Akte rechtfertigen". Solche Definitionen sind nach der Einschätzung von Menschenrechtsgruppen zu unpräzise und weitläufig, weil sie subjektiven Einschätzungen zu viel Gewicht verleihen. Künftig können derartige „Verdächtige" dazu gezwungen werden, ihre E-Mail-Adressen und alle ihre Zugänge (nicht aber die Passwörter) zu Twitter, Facebook und anderen sozialen Medien wie auch zu Forenkonten sowie zu Info- oder Administrationswebseiten preiszugeben (Pany, Frankreich: Parlament beschließt verschärftes Anti-Terrorgesetz, www.heise.de 03.10.2017; Ulrich, Freiheit, Gleichheit, Sicherheit SZ 19.10.2017, 6).

Großbritannien

Personalisierte Massenwerbung am Piccadilly Circus

Ca. 100 Mio. Menschen passieren pro Jahr den Piccadilly Circus in London. An der Kreuzung von Piccadilly, Shaftesbury Avenue und Regent Street befindet sich seit 1949 eine riesige 790 Quadratmeter große gewölbte Werbefläche, die bis Januar 2017 mit sechs Bildschirmen bestückt war. Nach einer längeren Warte- und Umbauzeit wurden diese nun durch einen einzigen Bildschirm ersetzt. Diese Piccadilly Lights sind künftig mit WLAN ausgestattet, das von den PassantInnen gratis genutzt werden kann. Außerdem kommt eine Erkennungstechnik zum Einsatz, die den Werbebildschirm in die Lage versetzt, auf seine Umgebung zu reagieren. Gemäß der Betreiberfirma Landsec erkennen versteckte Kameras rund um die Reklamefläche Marke, Modell und Farbe der vorbeifahrenden Autos, auf die abgestimmt dann Werbespots geschaltet werden. Zudem werden Alter und Geschlecht der FußgängerInnen gescannt und die Werbebotschaften hierauf angepasst (Menden, Versteckte Kamera, SZ 18.10.2017, 10).

Russland

Videoüberwachung in Moskau mit Gesichtserkennung

Die 170.000 Überwachungskameras der russischen Hauptstadt Moskau sollen nach dem Willen der Stadtverwaltung mit biometrischen Gesichtserkennung der Fa. N-Tech.Lab ergänzt werden. Ziel, so berichtet die Presse, sei es, Verbrecher ausfindig zu machen. Die russische Firma N-Tech.Lab hat auch die vor allem im sozialen Netzwerk vk.com zum Einsatz kommende Gesichtserkennungs-App FindFace entwickelt.

Die Zahl der in Moskau an öffentlichen Orten installierten Kameras ist vermutlich höher als in Großbritannien, das als Mutterland des Überwachungssystems CCTV (Closed Circuit Television) gilt. Ein Verband der britischen Sicherheitsindustrie schätzte 2013, dass die Regierung im ganzen Land rund 70.000 Überwachungskameras betreibe. In Moskau allein ist die Dichte der elektronischen Augen offenbar deutlich größer. Die Rede ist vom größten Überwachungsnetzwerk der Welt dieser Art.

Seit 2012 speichern die Behörden der russischen Hauptstadt Videomaterial aus den Kameras fünf Tage lang, sodass ständig rund 20 Millionen Stunden an Aufzeichnungen auf Festplatten liegen. Der IT-Beauftragte Moskaus, Artem Ermolaev, erklärte gegenüber der Presse: „Wir fanden rasch heraus, dass es unmöglich ist, solche Datenmengen allein von Polizisten durchsehen zu lassen“. Es läge daher nahe, die Suche nach Straftätern mithilfe von Künstlicher Intelligenz (KI) zu vereinfachen und zu verbessern.

Die zum Einsatz kommende Gesichtserkennungssoftware soll „digitale Fußabdrücke“ beziehungsweise Hashwerte von Bildern aus der Datenbank des russischen Innenministeriums zunächst mit Aufnahmen aus Eingängen zu größeren Wohnhäusern abgleichen. Ein zweimonatiger Test im ersten Halbjahr 2017 habe, so Ermolaev, dazu geführt, dass sechs Straftäter von einer bundesweiten Suchliste hätten verhaftet werden können. Nach und nach sollten Gesichtserkennungsfunktionen zunächst direkt in Kameras an Kriminalitätsschwerpunkten eingeführt werden. Alle auf einen Schlag mit der neuen Technik auszurüsten, hätte die bei ca. 72 Mio. € liegenden Wartungskosten pro Jahr verdreifacht.

Mikhail Zyuzin, ein IT-Experte von der Moskauer Akademie für Informationssysteme, erachtet den Schritt der Stadtverwaltung für legal, warnte aber vor Datenschutzrisiken. Sollte das System gehackt werden, könnten die Angreifer herausfinden, wo Betroffene wohnten, und Bewegungsprofile erstellen. Ermolaev versicherte dagegen, dass die Daten in einer geschlossenen Datenbank lägen und nur wenige Personen darauf Zugriff hätten. Zudem könne jeder aufmerksame Besucher von der Straße aus selbst feststellen, wer welche Mieter wann besuche (Krempl, Moskau ergänzt Videoüberwachung mit automatischer Gesichtserkennung, www.heise.de 29.09.2017).

USA

Datenbeschlagnahme im Ausland vor dem Supreme Court

Nachdem die US-Regierung bisher vergeblich versuchte Microsoft zu zwingen, in der EU gespeicherte Daten in die USA zu holen und preiszugeben, beschäftigt sich nun das höchste US-Gericht, der Supreme Court of the United States, mit dem Fall. Es geht dabei um die Frage, ob ein E-Mail-Provider in den USA einen US-Durchsuchungsbefehl auch dann umsetzen muss, wenn die Daten im Ausland gespeichert sind. Ausgangspunkt ist das seit 2013 laufende Verfahren USA v. Microsoft.

Ende 2013 hatte ein New Yorker Bundesbezirksgericht einen Durchsuchungsbeschluss erlassen, der Microsoft verpflichtete, E-Mails eines Kunden herauszugeben. Der Konzern überreichte einen Teil der Nachrichten, weigerte sich aber, auch auf Servern in Irland gespeicherte Daten auszuhändigen. Dafür seien irische Gerichte zuständig, meinte Microsoft. Die drei Richter des 2. Bundesgerichtsbezirk (2nd Circuit) entschieden als Berufungsgericht einstimmig gegen das Begehren der US-Regierung, da das zugrundeliegende Gesetz Stored Communications Act nur im Inland gelte. Daraufhin beantragte die US-Regierung eine erneute Anhörung vor einer erweiterten Richterbank desselben Gerichts. Nur vier von acht Richtern des 2nd Circuit stimmten für eine neuerliche Anhörung. Somit war dieser Antrag abgelehnt.

Daraufhin wandte sich die US-Regierung, unterstützt von 33 US-Staaten, an den Supreme Court. Dieser beschäftigt sich nur mit einem Bruchteil der an ihn herangetragenen Fälle. Meistens handelt es sich dabei um Rechtsfragen, die von Bundesberufungsgerichten uneinheitlich beantwortet wurden. Obwohl das hier nicht der Fall ist, haben die Höchstrichter den Fall angenommen, was darauf hinweist, dass sie die Angelegenheit für besonders wichtig erachten. Ein Termin für die mündliche Anhörung liegt noch nicht fest. Der Fall heißt offiziell „In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, United States of America v. Microsoft Corporation“ und trägt das Aktenzeichen 17-2 (Sokolov, US Supreme Court wird über US-Zugriff auf EU-Daten entscheiden, www.heise.de 17.10.2017).

USA

Justizministerium lockert Geheimhaltungspflicht bei Datenbeschlagnahme

US-Behörden sollen weiterhin im Geheimen auf Kundendaten zugreifen können, doch dürfen künftig die Anbieter die betroffenen Nutzenden hierüber zeitnah informieren. Nachdem dies Microsoft zugestanden wurde, hat das Unternehmen angekündigt, seine Klage in dieser Sache gegen das US-Justizministerium zurückzuziehen. In einem Memorandum hatte der Vize des US-Justizministers Rod Rosenstein öffentlich bekannt gegeben, dass Sicherheitsbehörden nur noch in Ausnahmefällen Kundendaten verlangen dürfen, ohne dass die Betreiber die betroffenen Kunden darüber zeitnah informieren dürfen. Das sei ein wichtiger Schritt für den Datenschutz und die Meinungsfreiheit, erklärte Brad Smith, Chef-Justiziar von Microsoft.

Microsoft hatte im Frühjahr 2016 Klage eingereicht, um sich das Recht zu erstreiten, eigene KundInnen über geheime Anfragen von US-Behörden nach ihren Daten zu informieren. Die Regelung würde gegen die US-Verfassung verstoßen. Unter Berufung darauf hatten US-Behörden „routinemäßig" die Herausgabe von Kundendaten verlangt und den Betreibern gleichzeitig untersagt, die betroffenen Kunden zu informieren. Teilweise enthielten diese Anordnungen keine Frist, so dass Betroffene nie von dem Datenzugriff erfuhren und damit beispielsweise auch keine Möglichkeit hatten, sich juristisch zu wehren. Jährlich habe das für Hunderte Verfügungen gegolten.

Smith erklärte, mit der nun vorgelegten Regeländerungen falle die Grundlage für das Gerichtsverfahren weg, weswegen man dessen Rücknahme einleite. Rosenstein hatte festgelegt, dass die geheimen Datenzugriffe besser begründet werden müssen und gegenüber den KundInnen zumeist nur noch maximal ein Jahr geheim gehalten werden müssen. Ausnahmen gelten demnach etwa bei einer Gefahr für die nationale Sicherheit. Microsoft begrüßt diese Änderung, fordert aber gleichzeitig vom US-Parlament, die gesetzliche Grundlage zu verbessern. Ein Gesetzentwurf dazu liege bereits auf dem Tisch (Holland, www.heise.de, Geheimer Datenzugriff für US-Behörden eingeschränkt – Microsoft zieht Klage zurück, www.heise.de 24.10.2017).

Indien

Kritik an Aadhar-Projekt

Der Aufbau der größten biometrischen Datenbank der Welt, des sog. Aadhar-Projektes, bei dem alle 1,3 Mrd. InderInnen per Iris-Scan und Fingerabdruck erfasst werden sollen und deren zwölfstellige Nummer zur Identifikation genutzt wird (DANA 3/2017, 172), bleibt in der Kritik. Mit Hilfe dieser Identifizierung sind viele Hundert Millionen InderInnen erstmals in der Lage, ein Bankkonto zu eröffnen, weil sie sich so ausweisen können. Zugleich steigt die Befürchtung, die zentral gespeicherten Daten könnten für Betrug und Identitätsdiebstahl zum Einfallstor werden, was in Indien häufig vorkommt. Der Streit verschärft sich, weil die Regierung ihre BürgerInnen zwingen möchte, sensible Daten wie Konto- und Telefonnummern in Aadhaar einfließen zu lassen. Wer sich dieser Forderung widersetzt, dem sollen ab 2018 das Konto und das Telefon gesperrt werden. Dagegen wurde vor dem Obersten Gericht ein Antrag eingereicht. In Jharkhand, einem der ärmsten indischen Bundesstaaten, erhielten kürzlich Familien ihre staatlichen Essensrationen nicht, weil die Beamten ihre Personalnummern nicht verifizieren konnten, nachdem das Internet ausgefallen war (Ohne Fingerabdruck kein Telefon, Der Spiegel 44/2017, 77).

Technik-Nachrichten

Massenhaft Datenschutzverstöße bei Kfz-Apps

Moderne Kraftfahrzeuge (Kfz) wissen oft viel über ihre FahrerInnen. Welche Daten über Fahrstrecken, Geschwindigkeit oder Bremsverhalten genau an die Kfz-Hersteller übertragen werden und was mit den Daten passiert, wird von diesen aber nicht verraten. Die Stiftung Warentest überprüfte 26 kostenlose Apps (Android und iOS) und stellte fest, dass die Programme alle mehr als nötig senden. Zudem weisen die Datenschutzerklärungen durchgängig deutliche Mängel auf.

Schon lange sind Fahrzeuge mit Sensoren ausgestattet, die z. B. Tempo, Bremsverhalten und Füllstände erfassen. Neu ist der Trend, dass immer mehr der Kfz laufend mit den Herstellern kommunizieren. Viele Modelle lassen sich per Bluetooth mit dem mit dem Internet verbundenen Smartphone koppeln. Oberklasse- und Elektro-Modelle verfügen zumeist bereits über einen Mobilfunkanschluss, über den sie sich mit Servern ihrer Hersteller verbinden.

Die Kommunikationsfreudigkeit moderner Autos soll den FahrerInnen Spaß und Komfort bieten: Mit der passenden App wird die Lieblingsmusik auf das Autoradio gestreamt, die nächste Werkstatt angezeigt oder eine auf dem Handy gespeicherte Adresse ins Navigationssystem eingegeben. Kfz mit eigener Sim-Karte lassen sich z. B. zwecks Diebstahlschutz aus der Ferne orten. Ihre BesitzerInnen können einzelne Funktionen vom Sofa steuern, zum Beispiel die Tür verriegeln oder die Standheizung einschalten. Handy und Kfz kommunizieren miteinander online über den Server des Herstellers, wobei eine Vielzahl von Daten anfällt.

Ein Auslöser für die Testreihe war der Fall eines Studenten, der im Mai 2016 vom Kölner Landgericht wegen fahrlässiger Tötung zu 33 Monaten Haft verurteilt worden ist, weil er einen Radfahrer überfahren hatte. Die entscheidenden Beweise lieferte sein Auto, ein Wagen des zu BMW und Sixt gehörenden Carsharing-Anbieters Drive Now. Nach Aufforderung durch das Gericht lieferte BMW die Daten, die Sensoren des Autos gesammelt hatten. Damit ließen sich Wegstrecke und gefahrene Geschwindigkeit genau rekonstruieren (DANA 4/2016, 201 f.).

Autos mit eigenem Mobilfunkanschluss sind derzeit noch selten auf deutschen Straßen. Mercedes etwa verbaut sie in der E-Klasse, BMW in der i-Reihe, Opel im neuen Astra und Mok-

ka, Ford und Toyota bislang gar nicht. Doch das wird sich bald ändern. Vom 31.03.2018 an müssen alle Neuwagen mit einem Notrufsystem über eine Mobilfunk-Sim-Karte ausgestattet sein. Es sendet bei schweren Unfällen automatisch eine Nachricht samt Standort an die Notrufzentrale. Über die Sim-Karte können auch andere Daten fließen, deren Schutz dann zu einem zentralen Thema wird. Wer über diese Daten verfügen darf, ist in Politik, Wirtschaft und Verbraucherschutz hoch umstritten.

- Der Test

Diese 13 Hersteller wurden getestet: Audi, BMW, Fiat, Hyundai, Mercedes-Benz (Daimler), Opel, Peugeot, Renault, Seat, Skoda, Tesla, Toyota, VW. Die Hersteller wurden ausführlich zu ihrem Umgang mit Daten befragt. Zudem wurde geprüft, was deren Handy-Apps versenden, indem diese Daten ausgelesen wurden. Es wurde sowohl für die Android- als auch für die iOS-Version der jeweiligen App geprüft, was diese wohin sendet, wenn NutzerInnen sie mit dem Auto verbinden oder sie daheim abseits des Pkw starten. Gab es mehrere Apps einer Automarke, wurde exemplarisch eine ausgewählt. Die Apps wurden auf einem Samsung Galaxy S8 oder iPhone 7 installiert und per Bluetooth mit passenden, von großen Mietwagenfirmen gemieteten Fahrzeugen verbunden. Getestet wurde von Mai bis September 2017. Die Hersteller wurden befragt, wie sie Kunden über Datenschutz aufklären, welche Daten sie online und offline erfassen, wo sie verarbeitet werden und ob sie sich löschen lassen.

Geprüft wurde außerdem, ob die Autohersteller die Nutzenden hinreichend darüber informieren, welche Daten die Apps verschicken und was damit geschieht. Die von Werkstätten genutzten Fehlerspeicher der Autos wurden ausgelesen und geprüft, ob diese sensible Daten wie den Standort erfassen.

Das ernüchternde Fazit der Untersuchung ist, dass der Datenschutz bei allen Herstellern mehr oder weniger auf der Strecke bleibt. Die Fragen von Stiftung Warentest beantwortete nur einer der Autobauer, nämlich Daimler. Selbst auf Nachfrage gab die fleißig Daten sammelnde Branche wenig über den Umgang mit diesen preis. Alle Apps sendeten mehr Daten als nötig. Die Nutzenden erfahren davon wenig. Klare, verständliche Datenschutzerklärungen liegen für keine der Apps vor. Selbst auf Nachfrage gibt die Branche, die so fleißig Daten sammelt, wenig über den Umgang mit ihnen preis.

- Datenübermittlung

Die Prüfung des Datensendeverhaltens ergab, dass alle Apps kritisch sind. Die meisten übermitteln nicht nur den Namen der NutzerIn, sondern auch die Identifikationsnummer des Fahrzeugs (FIN), also die „Fahrgestellnummer". Mit der FIN lässt sich u. a. der Erstkäufer des Autos ermitteln. Besser wäre es, die Apps würden für die Zuordnung zum Auto einen zufälligen Code als Pseudonym generieren.

Die übermäßigen Datenweitergaben widersprechen dem Grundsatz der Datensparsamkeit. Apps sollten nur solche Infos erheben, die für ihre Funktion nötig sind. Je mehr Details über Nutzende vorliegen, desto präzisere Profile lassen sich daraus erstellen.

Mithilfe eines dazwischen geschalteten Proxy-Servers wurden die Daten aus der App während der Fahrt ausgelesen, analysiert und, wenn nötig, entschlüsselt. Als kritisch beurteilt wurde, wenn Daten gesendet wurden, die für den Betrieb der App nicht notwendig waren, etwa die Geräte-ID des Smartphones, oder wenn zu präzise Daten erhoben wurden, die Rückschlüsse auf die Person zulassen können, wie z. B. die Fahrzeugidentifikationsnummer.

Ein Aspekt war es, wie aussagekräftig, vollständig und verbraucherfreundlich KundInnen über die Daten informiert werden, welche die Anwendung sendet. Dies bezieht sich sowohl auf die Informationen vor dem Herunterladen in Googles Play oder Apples App Store als auch auf die Infos nach der Installation der App. Ein Jurist prüfte deutschsprachige Datenschutzerklärungen auf Klauselverstöße. Fanden sich in den Stores und den Apps keine aussagekräftigen Dokumente zum Datenschutz, so lautete das Urteil „sehr deutliche Mängel". Wenn über den Datenschutz nur nach Installation der App aufgeklärt wurde, ebenso sofern Klauselverstöße gefunden, Sachverhalte wie Löschfristen nicht thematisiert wurden oder sich die Datenschutzerklärung nicht drucken ließ, so lautete das Urteil „deutliche Mängel".

Das Kfz-Diagnosesystem speichert Fehlercodes und Messwerte wie den Kilometerstand. Nur Daimler schickte den zugesendeten Fragebogen ausgefüllt zurück. Demgemäß können aktuelle Mercedes-Modelle „technische Daten" an das Unternehmen übertragen, etwa Füllstände, Reifendruck, Geschwindigkeiten. Der Konzern bietet KundInnen zudem einen Dienst, mit dem sie smarte Pkw orten können. Bewegungsprofile würden nicht erstellt. Daimler gibt zudem an, dass Daten auf deutschen Servern liegen. Externe Spezialisten würden die Server und auch internetfähige Autos auf Sicherheitslücken prüfen.

Audi, BMW und Tesla schickten lediglich Internet-Links oder allgemeine Infos zu ihren Datenschutzbestimmungen. Renault weigerte sich, an der Befragung teilzunehmen mit der Begründung, die Thematik sei zu komplex, um sie in einem Fragebogen in „für den Verbraucher verständlicher, transparenter Weise darzustellen". Keine Antworten auf die Fragen gaben trotz mehrere Nachfragen Fiat, Hyundai, Opel, Peugeot, Seat, Škoda, Toyota und Volkswagen.

Die Mehrheit der Kfz-Hersteller zeigte kein Verständnis für das Informationsbedürfnis der Verbraucherschützer. Wie berechtigt die Nachfragen sind, zeigt ein Blick auf die „Kundendatenschutzrichtlinie" des Elektroauto-Vorreiters Tesla auf seiner Website. Danach beziehen neben Tesla „möglicherweise" auch Dritte die Daten, etwa öffentliche Datenbanken, Marketingfirmen, Werkstätten und soziale Medien wie Facebook. Per Fernzugriff könne Tesla Daten zum Fahrstil sowie Videoaufnahmen von Fahrzeugkameras sammeln. Die Infos könnten bei Dritten landen, im Falle einer Ermittlung auch bei Behörden. Arbeitnehmer werden besonders adressiert: „Wir können Informationen (...) an Ihren Arbeitgeber weitergeben (...), wenn das Produkt nicht Ihnen selbst gehört und sofern dies nach geltendem Recht zulässig ist."

Die Testenden konnten nicht prüfen, was Autos mit eingebauter Sim-Karte übertragen: Es war technisch nicht möglich, sich in die Mobilfunkver-

bindung der verbauten Sim-Karte zu hacken. Die von den Handy-Apps der Autobauer gesendeten Daten wurden dagegen ausgelesen. Die meisten übermitteln den Namen des Nutzers und die FIN. Google und Apple sowie teilweise weitere Stellen erfahren nach dem Start den Standort, unabhängig davon, ob der Nutzer navigiert oder nur Musik hört. Selbst Anwendungen mit beschränkten Funktionen bespitzeln die Nutzenden, etwa die Service-App von Fiat, die heimlich mit Facebook kommuniziert. Audi MMI connect schickt Infos sogar unverschlüsselt.

Gemäß dem Bundesdatenschutzgesetz (BDSG) sowie dem Telemediengesetz (TMG) dürfen personenbezogene Daten nur erhoben werden, wenn die betroffene Person eingewilligt hat. Um einwilligen zu können, muss sie vor Installation der App über die Datensammelei aufgeklärt werden, und zwar umfassend und verständlich. Das leistet keiner der geprüften Anbieter.

Peugeot und Renault haben im Google Play Store Dokumente nur auf Französisch hinterlegt und in den Apps selbst gar keine. Auch die anderen Apps offenbaren erhebliche Mängel. Meist sind die Erläuterungen zum Datenschutz schwer zu finden oder schwammig formuliert. Kurzfassungen zu den wichtigsten Datenschutzfragen, wie sie das Bundesjustizministerium fordert, konnten nirgends gefunden werden.

Das Fazit von Stiftung Warentest ist: Kfz-Fahrende, die vor Schnüffelei sicher sein wollen, sollten auf Hightech verzichten. Mit älteren Wagen fährt man noch weitgehend inkognito (Schnüffler an Bord, test 10/2017, 70-75).

Stiftung Warentest: Kamera-Apps von Yi und Sony übermitteln ins Ausland

Kamera-Apps verraten teilweise nicht bekannten Stellen sensible Informationen über die Nutzenden. Die Stiftung Warentest hat untersucht, welche Daten die Software an ihre Schöpfer weitergibt. Getestet wurden die Apps der namhaften Kamera-Anbieter Canon, Fujifilm, Nikon, Olympus, Panasonic, Ricoh, Sony und Yi, jeweils Android- und iOS-Versionen. Dabei zeigte sich, dass Sony und Yi im Hintergrund weit mehr machen, als mancher FotografIn lieb sein dürfte.

Yi Technology heißt der Anbieter der ersten spiegellosen Systemkamera aus China, der Yi M1, der für sich wirbt: „Die am besten vernetzte spiegellose Kamera der Welt“. Er liefert dazu die kostenlose Yi Mirrorless-App. Sie dient in erster Linie zum bequemen Teilen der Fotos in sozialen Netzwerken wie Facebook. Eine für viele Fotografen hilfreiche Fernsteuerung der Kamera ist in der Mirrorless App nicht vorgesehen. Hilfreich ist die Software aber für den Anbieter, indem sie ihm eine Menge persönlicher Daten des Anwenders liefert: Die Gerätekennungen seines Smartphones und seiner Kamera, aber auch Namen und Kennwort der drahtlosen Netzwerkverbindung zwischen Kamera und Smartphone, was technisch absolut überflüssig ist.

Die Yi-App schickt ihre Daten an chinesische Server. Ein anderer Teil ihres Datenstroms landet bei Unternehmen wie Facebook und Google in den USA, ohne dass hierfür ein Grund erkennbar wäre. Um Fotos in sozialen Medien zu teilen, werden die Daten nicht gebraucht. Der Anwender erfährt nichts von diesen Datenweitergaben. Die App gibt keinen Hinweis und fragt nicht um Erlaubnis. Eine Möglichkeit, der Übertragung zu widersprechen, fehlt. Das ist gemäß deutschem Datenschutzrecht eindeutig unzulässig.

Nur bei Sony verhält es sich ähnlich kritisch: Die Foto App „PlayMemories Mobile“ sendet Infos zur verwendeten Kamera und zum Mobilfunk-Anbieter an Sony. Standortdaten gehen an Google, bei der iOS-Version an Apple. Weniger mitteilungsbedürftig, aber ebenfalls kritisch sind die Apps Fujifilm Camera Remote (Android), Nikon SnapBridge (iOS) und Olympus Image Share. Sie verraten den Standort des Anwenders. Gar keine persönlichen Daten erfassen Canon Camera Connect, Fujifilm Camera Remote (iOS), Panasonic Image App, Ricoh Image Sync und Nikon SnapBridge (Android).

Die Nutzenden sollten daher darauf achten, welche Zugriffsberechtigungen die Foto-App anfordert. Nach Möglichkeit sollte der Weitergabe von Kamera- und Standortdaten widersprochen werden, was allerdings nicht immer funktioniert. Weitgehend unkritisch erwiesen sich die Apps von Canon, Fujifilm, Nikon, Panasonic und Ricoh. Sony greift dagegen kombinierte Kamera- und Standortdaten ab. Als richtige Datenschleuder entpuppte sich die Yi Mirrorless App, die ungefragt und ohne erkennbaren Grund persönliche Gerätedaten, Netzwerknamen und Kennwort an chinesische Server sendet (Kamera-Apps und Datenschutz: Yi funkt persönliche Daten nach China, www.test.de 05.09.2017).

Sicherheitslücken bei „Smart Toys“

Immer häufiger finden sog. Smart Toys in Gestalt von Plüschtieren, Kätzchen, Teddys, Puppen oder auch Robotern den Weg in heimische Kinderzimmer. Die Stiftung Warentest hat sieben mithörende Spielzeuge und ferngesteuerte Roboter untersucht und dabei gefährliche Sicherheitslücken entdeckt. Drei der getesteten Spielzeuge benötigen für eine Bluetooth-Verbindung weder ein Passwort noch einen PIN-Code. Jeder Smartphone-Nutzende könne sich auf diese Weise mit den Spielwaren verbinden, „um das Kind abzuhören, es auszufragen oder zu bedrohen“. Dafür seien weder Hackerkünste noch der physische Zugriff auf das Spielzeug notwendig. Mit dem Roboter von i-Que können Fremde etwa aus der Nachbarwohnung dem Kind Anweisungen geben; die Antworten des Kindes lassen sich abhören.

Mit dem smarten Teddy von Toy-Fi können Eltern ihrem Kind Sprachnachrichten schicken, allerdings auch Fremde. Der bellende Roboterhund Wowwee Chip kostet immerhin etwa 220 Euro. Er lässt sich von jedem Smartphone aus steuern, also auch von Unbefugten. Zudem gibt er Informationen zum genutzten Smartphone an Drittanbieter weiter. Bei den vier als kritisch eingestuften Spielzeugen, darunter die „Hello Barbie“ von Mattel und einem Roboter-Dino für 300 Euro, fand die Stiftung Warentest zwar keine unsicheren Funkverbindungen, jedoch problematisches Ausspähverhalten bei den dazugehö-

renden Apps. So erfassen einige die Geräte-ID des Smartphones oder senden Namen und Geburtsdatum des spielenden Kindes an den Anbieter. Manche setzen Tracking-Programme ein, mit denen auch das Surfverhalten der Eltern mitgeschnitten werden kann. Einige verhielten sich wie „Spione im Kinderzimmer“: Sie nehmen über integrierte Mikrofone die Gespräche der Kinder auf und schicken sie an die Server der Anbieter. Bei der Barbie lässt sich das eigene Kind belauschen, Eltern können laut Stiftung Warentest alle Sprachaufnahmen des Kindes online abhören.

Die Grünen-Politikerin Renate Künast, Vorsitzende des Ausschusses für Verbraucherschutz im deutschen Bundestag in der 18. Legislaturperiode, kommentierte: „Das Kinderzimmer darf kein Einfallstor für Ausspähung sein.“ Kinder seien besonders schutzbedürftig. Aus einer Antwort der Regierung auf eine Anfrage der Grünen geht hervor, dass die Bundesnetzagentur bereits 160 Verfahren eingeleitet und 400 Angebote gelöscht habe, weil diese illegale Spionagegeräte seien. Eines davon war die smarte Puppe „My friend Cayla“, die Anfang des Jahres verboten und damit aus dem Handel genommen werden musste (DANA 1/2007, 42 ff.). Künast forderte, dass gegen den Roboter von i-Que vorgegangen wird. Die Bundesnetzagentur sah dafür aber keinen Grund, weil viele Händler den Roboter nicht mehr im Sortiment hätten. Auch Caylas Konkurrentin „Hello Barbie“ darf wohl weiter mit Kindern spielen. Sie sei juristisch gesehen keine versteckte Spionage-Anlage, weil die Aufnahmefunktion erkennbar ist: Kinder müssen dafür einen Knopf an ihrem Gürtel gedrückt halten (Hauck, Das Kuscheltier hört zu, SZ 30.08.2017, 15 = Spione im Kinderzimmer, www.sueddeutsche.de 29.08.2017).

Uber-App ermöglichte Screenshots

Der Fahrdienstvermittler Uber hat eingeräumt, dass seine iPhone-App in der Lage ist, ohne Wissen der Nutzenden Screenshots anzufertigen, selbst wenn die App geschlossen ist. Den zugehörigen Code will das Unternehmen nun aus der App entfernen. Entdeckt wurde die Funktion vom Sicherheitsforscher Will Strafach. Ihm zufolge nutzt Uber eine nicht dokumentierte App-Berechtigung, die den Zugriff auf die Screenshot-Funktion gewährt. Es sei eine von mehreren Berechtigungen, die normalerweise EntwicklerInnen nicht zur Verfügung ständen, außer Apple räume ihnen diese spezielle Berechtigung gesondert ein. Strafach geht davon aus, dass Uber die einzige App eines Drittanbieters ist, die von Apple die Berechtigung zur Aufzeichnung von Screenshots im Hintergrund erhalten hat. Bei einer Analyse von Tausenden Apps habe er die Berechtigung nur bei Uber gefunden.

Auch andere App-Entwickler erklärten gegenüber ZDNet USA, ihnen seien keine weiteren Beispiele bekannt. Der Apple-Experte und Jailbreak-Autor Luca Todesco sprach von einem „extrem gefährlichen“ Einzelfall. Die Berechtigung „com.apple.private.allow-explicit-graphics-priority“ erlaube es einem Entwickler, den Framebuffer eines iPhones zu lesen und zu schreiben. Der Framebuffer ist ein Teil des Arbeitsspeichers, der Informationen zu jedem Pixel des Displays und weitere Daten enthält. Die Schreibberechtigung stehe jeder App über den normalen Rendering-Service zur Verfügung. Die Leseberechtigung bedeute, dass eine App jederzeit auf den Bildschirm schauen könne: „Das ist so, als würde man einer App eine Keylogging-Funktion geben“. Die spezielle Berechtigung versetze die Uber-App auch in die Lage, die Anmeldedaten von Nutzenden zu nutzen, so Todesco: „Ich finde das sehr beängstigend und gefährlich“.

Ein Uber-Sprecher erklärte, der Code sei nur benutzt worden, um das Rendering der Uber-App auf der Apple Watch zu verbessern. Die zu der Screenshot-Berechtigung gehörende Programmierschnittstelle ermögliche es der App, Karten auf einem iPhone im Hintergrund zu rendern und dann an die Apple Watch zu senden. Der Code und die API würden nun vollständig entfernt (Beiersmann, Uber-App macht auf iPhones heimlich Screenshots, www.silicon.de 06.10.2017).

Rechtsprechung

OVG Nordrhein-Westfalen

Fahrerbewertung im Internet unzulässig

Das Oberverwaltungsgericht (OVG) Münster hat in zweiter Instanz das Angebot eines Internet-Prangers gegen Raser und Drängler, das Portal Fahrerbewertung.de, mit Urteil vom 19.10.2017 für rechtswidrig erklärt (Az. 16 A 770/17). Darüber können Menschen, die das Verkehrsverhalten anderer Kfz für unangemessen ansehen, unter Eingabe des Autokennzeichens das Fahrverhalten mit den Farben Rot, Gelb oder Grün bewerten, hier also mit Rot brandmarken

Dieser Zeitvertreib unserer mobilen Gesellschaft versprach den Betreibern der Seite viel Traffic und Werbeeinnahmen. Diese beteuerten indes hehre Absichten: Man wolle die FahrerInnen mittels schlechter Noten zur „Selbstreflexion“ anhalten und dadurch zur Sicherheit im Straßenverkehr beitragen. Wer sich dafür interessiert, ob der freundliche Nachbar oder Kollege auch auf der Autobahn ein netter Mensch ist, könne mal schnell die Autonummer eintippen. Die Datenschutzbeauftragte Nordrhein-West-

falens (LDI NRW) war wenig begeistert und machte dem Portal Auflagen. Insbesondere sollte der allgemeine Zugang zu den Bewertungen untersagt sein. Es brauche keine „Nebenjustiz" in Form einer privaten Verkehrssünderkartei.

Es ging zunächst um die Frage, ob Autonummern überhaupt „personenbezogene Daten" sind. Das wurde von den Klägern in Frage gestellt, weil NormalautofahrerInnen kaum an den Namen hinter der Nummer gelangen könnten. Schon gemäß der Darstellung der Vorinstanz, des Verwaltungsgerichts (VG) Köln, das den Datenschützern in erster Instanz recht gegeben hatte, ist das Nummernregister ein offenes Buch: Letztlich müsse man dem Kraftfahrt-Bundesamt nur ein „rechtlich relevantes Interesse", z. B. eine Schramme im Blech, vorspiegeln, und schon bekomme man den gewünschten Namen.

Die Betreiber mussten nun auch in zweiter Instanz eine Niederlage einstecken. Das OVG stellte fest, dass das Portal tief in das Recht auf Datenschutz eingreift, weil „eine vollständig anonyme Bewertung von in der Regel privat motiviertem Verhalten für eine unbegrenzte Öffentlichkeit einsehbar" ist. Die Richter hielten also missbräuchliche Bewertungen für wahrscheinlich. Diese könnten für die Betroffenen negative Konsequenzen haben: Arbeitgeber oder Versicherungen könnten sich für die Bewertungen interessieren. Fraglich ist zudem, ob der Datenpranger wirkliche Übeltäter dazu veranlasst, den Fuß vom Gaspedal zu nehmen. Hierfür müssten sie erst einmal davon erfahren. Gemäß der Verfügung der LDI NRW sind übrigens Fahrer-Bewertungen nicht in jedem Fall ausgeschlossen. Doch soll die FahrzeughalterIn die Einzige sein, die von der Note Kenntnis erlangen darf. Nach Ansicht des OVG könne dies genügen, um zur „Selbstreflexion" anzuhalten. Eine Revision gegen das Urteil wurde nicht zugelassen (Janisch, Ausgebremst, SZ 20.10.2017, 1).

AG München

Bußgeld wegen Kfz-Dashcam mit Daueraufzeichnung

Das Amtsgericht (AG) München hat mit Urteil vom 09.08.2017 gegenüber einer 52-jährigen Frau ein Bußgeld in Höhe von 150 € verhängt, weil sie mit Dashcam-Aufnahmen die Schuldigen für Sachbeschädigungen an ihrem parkenden Fahrzeug dokumentieren wollte (1112 OWi 300 Js 121012/17). Es bewertete dies als eine unbefugte Erhebung personenbezogener Daten und damit als einen Verstoß gegen das Bundesdatenschutzgesetz (BDSG). Die Frau hatte im August 2016 ihren BMW für drei Stunden in einer Münchner Straße abgestellt; währenddessen machten dem Gericht zufolge vorn und hinten am Wagen angebrachte Dashcams Aufnahmen. Mindestens drei andere Fahrzeuge seien während der Zeit gefilmt worden. Ein Fahrzeug streifte und beschädigte ihr Auto. Die Frau gab die Videoaufnahmen als Beweismittel an die Polizei – und handelte sich damit einen Bußgeldbescheid ein. Sie legte Einspruch gegen den Bescheid ein, weil bei den Aufnahmen keine Fahrer zu erkennen und Autokennzeichen keine schützenswerten Daten seien.

Das AG entschied, dass „das Recht der gefilmten Personen auf informationelle Selbstbestimmung" das Interesse der Betroffenen an der Aufdeckung einer potenziellen Straftat überwiegt: „Nach Auffassung des Gerichtes überwiegt hier im vorliegenden Fall das Recht der gefilmten Personen auf informationelle Selbstbestimmung. Das Interesse der Betroffenen an der Aufdeckung von einer potentiellen Straftat muss hierbei zurückstehen. Das permanente anlasslose Filmen des vor und hinter dem geparkten Fahrzeug befindlichen Straßenraums verletzt das Recht auf informationelle Selbstbestimmung und stellt einen schwerwiegenden Eingriff in dieses Recht dar. Es geht nicht an, dass 80 Millionen Bundesbürger mit Kameras herumlaufen, um irgendwelche Situationen aufnehmen zu können, die eine Straftat aufdecken könnten. Eine permanente Überwachung jeglichen öffentlich Raumes durch Privatbürger ist nicht zulässig, da es in das Recht unbeteiligter Personen in schwerwiegender Weise eingreift, selbst bestimmen zu können, wo und wann man sich aufhält, ohne dass unbeteiligte Personen dies dokumentieren und bei Behörden verwenden würden." Bei der Bußgeldhöhe hat das Gericht berücksichtigt, dass die Betroffene nur 1.500 Euro netto verdient. „Zu ihren Gunsten konnte gewertet werden, dass offenbar in der Vergangenheit das Fahrzeug schon einmal beschädigt worden ist und die Betroffene subjektiv einen Anlass hatte, die Kameras einzusetzen".

Die Frage, ob und wie Videoaufnahmen von Dashcams in gerichtlichen Verfahren verwendet werden dürfen, ist bisher höchstrichterlich nicht entschieden. Das OLG Stuttgart bejahte die Frage der Verwertbarkeit von Kfz-Kameraaufnahmen. Zuvor hatte das Landgericht Rottweil die Nutzung genau dieses Materials nicht zugelassen, weil es die Selbstbestimmungsrechte der Gefilmten verletze. Die Bundesbeauftragte für den Datenschutz hatte davor gewarnt, Verkehrsgeschehen mit Dashcams aufzuzeichnen, weil das datenschutzrechtlich nicht zulässig sei (Kannenberg, Geldbuße wegen Dashcam-Einsatz im Auto, www.heise.de 02.10.2017; Überwachungskamera im Auto verboten; SZ 04.10.2017, 26; Das Auto im Fokus, Pressemitteilung 76 vom 02.10.2017, www.justiz.bayern.de).